NUMER 1/2022
ISSN 2720-6513

PRZYSZŁOŚĆ ZACZYNA SIĘ DZISIAJ

Domena

Nowa odsłona cyberwojny

Drony w natarciu

Mistyczny wymiar metawersum

MICHAŁ OGÓREK
Z UKOSA

NIE DAJMY SIĘ SKOPAĆ PEGAZOWI

Spis treści

Domena
PRZYSZŁOŚĆ ZACZYNA SIĘ DZISIAJ

nr 1/2022

Wydawca:
Polskie Towarzystwo Informatyczne

Zarząd Główny:
Ul. Solec 38 lok.103
00-394 Warszawa
NIP: 522-000-20-38
tel: +49 22 838 47 05
E-mail: pti@pti.org.pl

Redaktor naczelna:
Anna Kniaź
(anna.kniaz@pti.org.pl)

Rada Programowa „Domeny":
Wiesław Paluszyński
– przewodniczący Rady
Marek Bolanowski
Marian Bubak
Beata Chodacka
Bogusław Dębski
Wojciech Kiedrowski

Współpraca redakcyjna:
Tomasz Kulisiewicz

Korekta:
Jolanta Jamiołkowska

Skład i opracowanie graficzne:
Agencja HEADOUT

Headout

Szanowni Państwo,

przed ponad rokiem Biuletyn PTI przeszedł metamorfozę, ewoluując w stronę pisma informatycznego, co spotkało się z dobrym przyjęciem. Apetyt rośnie w miarę jedzenia, więc uznaliśmy, że pora na bardziej zasadnicze zmiany – i formuły, i tytułu. Szukając inspiracji dla nowego szyldu, skupiliśmy się na określeniu tych obszarów, które zawsze były domeną naszego stowarzyszenia – stąd nowy tytuł kwartalnika PTI.

Nasza domena – informatyka – nieustannie ewoluuje i ma przemożny wpływ na całą cywilizację. Chcemy się tej dominacji przyglądać nie tylko z powodu właściwego informatykom poczucia odpowiedzialności za świat, który wykreowali. Społeczne implikacje rozwoju IT są naprawdę fascynujące, dlatego na łamy „Domeny" zaprosiliśmy antropologa technologii, a w następnych numerach – w nowym dziale: Informatyka i antroposfera – będziemy publikować wiele interesujących treści związanych z mediami elektronicznymi i kulturą cyfrową.

Informatyka ma także – choć w polskich realiach chyba bezpieczniej napisać, że powinna mieć – ogromy wpływ na edukację. W PTI bardzo prężnie działa Sekcja Informatyki Szkolnej, grupująca nauczycieli entuzjastów, i na łamach „Domeny" stworzyliśmy im dodatkową przestrzeń do wymiany doświadczeń edukacyjnych. W dziale Informatyki szkolnej tego numeru „Domeny" specjaliści dzielą się pomysłami na sensowne nauczanie informatyki w szkołach i kreatywne używanie narzędzi TIK.

Te nasze plany edytorskie, podobnie jak większość dotąd elektryzujących nas zamierzeń, znienacka zmroziła wojna. Zdyskredytowała wagę wielu wybranych tematów. Dobrym przykładem może być Pegasus – na szczęście dla „Domeny" sposób działania systemu technologicznie się nie zmienił, ale z politycznego punktu widzenia temat przestał istnieć, mimo że pod koniec marca br. w PE powstała komisja śledcza, do której trafiło aż 8 europosłów z Polski, a koordynatorką prac z ramienia frakcji, która zainicjowała powstanie komisji, jest nasza krajanka – Róża Thun.

Wojna wprowadza inną hierarchię spraw. Rozprasza także uwagę, niezwykle trudno jest kreować nowe treści, gdy – przejęci zgrozą – cały czas nasłuchujemy wieści z frontu. Nie spodziewałam się, że pierwszy numer „Domeny" będzie otwierał nowy dział opatrzony dramatycznym hasłem: IT na wojnie. Pozostaje mieć nadzieję, że za kwartał będziemy mogli powitać naszych czytelników bardziej optymistycznym przesłaniem.

Anna Kniaź
redaktor naczelna

Nowa odsłona cyberwojny

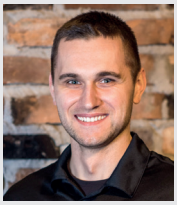
Nie epatujmy nagłaśnianymi medialnie atakami grupy Anonymous. Prawdziwa cyberwojna Rosji z Ukrainą toczy się w tle od kilku lat, a wielu jej aspektów możemy nigdy nie poznać.

Podczas aneksji Krymu w 2014 r. Rosjanom udało się sparaliżować nie tylko ukraińskie sieci telekomunikacyjne, lecz także system dowodzenia i kierowania obroną państwa. Od tej pory kolejne spektakularne cyberataki miały być dowodem na supremację Rosji w cyberprzestrzeni. W grudniu 2015 r. hakerzy rosyjscy włamali się do ukraińskich systemów informatycznych kontrolujących sieci energetyczne i na 6 godzin wyłączyli zasilanie, pozostawiając setki tysięcy Ukraińców bez prądu. Jak później ustalili analitycy, za tym czysto politycznym zadaniem stały służby rosyjskiego wywiadu. Rok później doszło do powtórki, tym razem tylko Kijów został pozbawiony prądu. Apogeum przyszło rok później, gdy rosyjska cyberarmia została wzmocniona o narzędzia, wykradzione z amerykańskiej agencji wywiadowczej National Security Agency (NSA).

NotPetya sieje zniszczenie

– 27 czerwca 2017 r. Kreml odpalił cyberbroń NSA na Ukrainie, co okazało się najbardziej destrukcyjnym i kosztownym cyberatakiem w historii świata. Tego popołudnia zgasły ekrany wszystkich urządzeń na terenie kraju. Ukraińcy nie mogli pobrać gotówki z bankomatu, zapłacić za paliwo na stacji benzynowej, wysłać lub odebrać maila, kupić biletu na pociąg, zrobić zakupów spożywczych, odebrać własnego wynagrodzenia oraz, co najgorsze, monitorować poziomu promieniowania radioaktywnego w elektrowni w Czarnobylu. Konsekwencje ataku odczuwalne były także poza granicami Ukrainy. Ucierpiały firmy prowadzące działalność na terenie tej byłej radzieckiej republiki. Każdy ukraiński pracownik międzynarodowej organizacji stanowił furtkę do

Swoją wiedzą podczas marcowego Klubu Informatyka podzielili się wybitni specjaliści w zakresie cyberbezpieczeństwa:



Rafał Chruściel

analityk zagrożeń oraz inżynier bezpieczeństwa infrastruktury IT, od 10 lat związany z branżą cyberbezpieczeństwa. Doświadczenie zdobywał w takich firmach, jak F5 Networks czy Allegro. Obecnie lider zespołu reagowania na incydenty w ISS World Services A/S.

Łukasz Jachowicz

specjalista ds. cyberbezpieczeństwa w Mediarecovery, prezes Internet Society Poland. Zawodowo zajmuje się analizą incydentów bezpieczeństwa, cyberbezpieczeństwem ofensywnym oraz doradzaniem w kwestiach zabezpieczania infrastruktury. Był członkiem Rady ds. Cyfryzacji. Wieloletni doradca największych firm technologicznych.

sieci globalnej. Zaatakowano komputery spółek farmaceutycznych Pfizera oraz Mercka, gigantów na rynku przewozów i dostaw, czyli firm Maersk oraz FedEx, jak również producenta wyrobów czekoladowych Cadbury w jego fabrykach zlokalizowanych na Tasmanii – pisze Nicole Perlroth w prologu do swojej niedawno wydanej książki: „Cyberbroń i wyścig zbrojeń. Mówią mi, że tak kończy się świat", uznanej przez Financial Times & McKinsey za najlepszą książkę biznesową roku 2021.

Skutki ataku były niewiarygodnie dotkliwe. Gigantowi morskiemu Maersk, operującemu 800 statkami w 76 portach, przywrócenie systemu na 4 tys. serwerów oraz 45 tys. komputerów zajęło dwa tygodnie i wymagało zaangażowania 600 specjalistów. Operacja się powiodła, bo dzięki awarii zasilania w Ghanie ocalała jedyna niezainfekowana kopia danych. Straty Maerska oszacowano na 1 mld USD.

Chwile grozy przeżył personel elektrowni w Czarnobylu, gdy utracono możliwość kontroli promieniowania. Siergiej Gonczarow, kierownik techniczny elektrowni w Czarnobylu, po zorientowaniu się co do skali ataku, nakazał fizyczne odłączenie komputerów i wysłał pracowników, aby na zewnątrz ręcznie dokonywali pomiarów promieniowania.

Preinwazyjne cyberataki

W tym roku Rosji marzyła się powtórka z 2014 – wywołanie chaosu w Ukrainie za pomocą cyberataków, poprzedzających inwazję militarną. W nocy z 13 na 14 stycznia br. Rosja przypuściła szturm na wiele ukraińskich serwisów rządowych, podmieniając treści (tzw. deface) na taki obrazek:

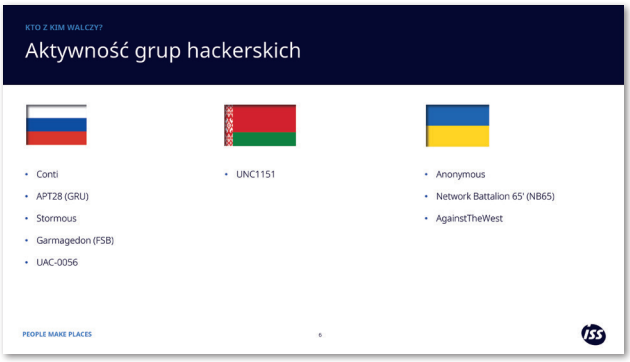
– CERT ukraiński obwinił za to działanie grupę białoruską. W ramach działań dezinformacyjnych na przejętych stronach pojawił się tekst w trzech językach, w tym w dość kulawej polszczyźnie, co zapewne było próbą wskazania fałszywego tropu do Polski. Dzień później zidentyfikowano ransomware WhisperGate, a 8 lutego CERT UA odkrywa farmę botów we Lwowie (18 tys. fałszywych kont w mediach społecznościowych), mającą za zadanie sianie paniki wśród ludności ukraińskiej. 15 lutego przypuszczono ataki DDoS na ukraińskie strony rządowe, za atakami stało najprawdopodobniej GRU. Tego samego wykonano atak typu spear phishing na sektor mediowy i militarny, za co odpowiedzialna była związana z FSB rosyjska grupa Garmagedon. Wreszcie 23 lutego zidentyfikowano HermeticWiper – informował Rafał Chruściel, analityk zagrożeń i inżynier bezpieczeństwa infrastruktury IT podczas Klubu Informatyka, zorganizowanego pod koniec marca br. przez Mazowiecki Oddział PTI.

HermeticWiper zaatakował setki maszyn w Ukrainie, ale nie wyrządził szkód o oczekiwanych rozmiarach z dwóch powodów: Ukraina od 2014 r. zdołała poprawić swoje zabezpieczenia i tym razem miała wsparcie sojuszników.

Słowacka firma ESET, zajmująca się cyberbezpieczeństwem, odkryła mechanizm ataku i poinformowała o nim społeczność międzynarodową (prawdopodobnie w celu zmylenia programów antywirusowych Wiper jest podpisany przy użyciu certyfikatu podpisywania kodu wydanego przez cypryjską firmę Hermetica Digital Ltd, stąd nazwa tego malware). Znacznik czasowy kompilacji PE jednej z próbek wskazuje na to, że atak mógł być przygotowywany już od końca 2021 r. Równie szybko zareagował Microsoft (HermeticWiper bierze na cel systemy operacyjne rodziny Windows) i zawiadomił amerykańskie służby.

Wojna dzieli Internet

Liczba grup hackerskich walczących po każdej ze stron konfliktu zmienia się płynnie, proporcja liczbowa wskazuje na przewagę ukraińską, według https://twitter.com/cyberknow20 4 kwietnia br. były to 23 grupy prorosyjskie, 48–51 proukraińskich (nie tylko z Ukrainy). Prorosyjskie grupy są sponsorowane przez rząd, wywiad i FSB, proukraińskie to aktywiści sympatyzujący z Ukrainą. W ramce zamieszczamy zestawienie najbardziej znanych grup walczących po obu stronach, ta pod flagą białoruską jest sponsorowana przez Rosję.



Dwa dni po inwazji Mychajło Fedorow, ukraiński wicepremier i minister transformacji cyfrowej wezwał za pośrednictwem Telegramu do utworzenia cyberarmii Ukrainy. ITArmy, organizująca swoje działania za pośrednictwem szyfrowanych kanałów w Telegramie, ma być dobrowolną, ale oficjalną instytucją rządu Ukrainy. Trudno jednak zweryfikować, w jakim stopniu ta inicjatywa się powiodła. Niewątpliwie Ukraina zaczęła się bronić, przeprowadzając kontruderzenia. W miarę trwania inwazji ataki obu stron się intensyfikują i obecnie mamy do czynienia z cyberwojną na pełną skalę.

– *W dniu inwazji militarnej przeprowadzono ataki DDoS na rosyjskie strony rządowe. W odwecie dzień później sponsorowana przez rząd białoruski grupa UNC1151 rewanżuje się atakami phisingowymi na Ukrainę. Conti gang ogłasza wsparcie dla Rosji, po czym jeden z ukraińskich badaczy bezpieczeństwa, najprawdopodobniej członek gangu, publikuje 60 tys. wiadomości wymienionych między członkami grupy. 26 lutego NB65 hakuje Instytut Badań Jądrowych Rosyjskiej Akademii Nauk i publikuje 40 tys. plików, ale nie analizowałem ich zawartości* – informował Rafał Chruściel. Koleje Białoruskie po ataku Anonymous przechodzą na ręczne sterowanie, odnotowując ogromne opóźnienia na stacjach kolejowych. 1 marca kolejny malware: IsaacWiper oraz HermeticRansom zostają odkryte w Ukrainie.

2 marca powiązana z Anonymous NB65 atakuje Roskosmos - rosyjskie NASA. Pięć dni później ATP28 powiązana z wywiadem rosyjskim przeprowadza atak na ukraińską grupę mediową UkrNet, białoruski UNC1151 uruchamia kampanie phishingowe w Polsce i Ukrainie. Dzień później RuRansom szyfruje dane na komputerach, na których zostaje uruchomiony, nie żąda jednak okupu, wyświetla info o działaniach Putina. 10 marca pojawia się Liberator – fake narzędzie do DDoS, tak naprawdę trojan, szpiegujący i wysyłający dane na rosyjskie adresy. W połowie marca pojawił się fake translator z języka ukraińskiego, kierowany głównie do osób przekraczających granicę ukraińsko-polską i ukraińsko-węgierską. 22 marca zaczął działać DoubleZero wiper.

Techniki ataków obu stron są podobne:

Target: **Ukraina**	Target: **Rosja**
DiskWiping: WhisperGate, HermeticWiper, DoubleZero, CaddyWiper, IsaacWiper	Ransomware: RuRansom
Defacement	DDoS
Fake News	Defacement
Spear Phishing	Data leakage
	Fake News

Źródło: Prezentacja Rafała Chruściela

– *Głównym narzędziem wojny informacyjnej są fake newsy, pojawiła się ich ogromna liczba. Coraz częściej dochodzi do wykorzystywania technologii deep fake* – mówił Rafał Chruściel, demonstrując zmanipulowane wystąpienie prezydenta Zełenskiego.

#OpRussia

Zaledwie kilka godzin po zbrojnym ataku Rosji kolektyw hakerski Anonymous wypowiedział wojnę Rosji na Twitterze. Od tego czasu pod hasztagiem #OpRussia publikowane są zrzuty ekranowe zhakowanych stron internetowych rosyjskich stacji radiowych lub stron rządowych, filmiki o wyciekach danych, wykradzione pliki, a nawet podsłuchy komunikacji rosyjskiego wojska.

Rafał Chruściel postrzega Anonymous jako grupę haktywistów przeprowadzających ataki cybernetyczne bez celów finansowych, najczęściej są one wyrazem manifestacji obywatelskiej niezgody. Drugi z ekspertów zaproszonych na Klub Informatyka – Łukasz Jachowicz – specjalista ds. cyberbezpieczeństwa w Mediarecovery i prezes Internet Society Poland, postanowił przeanalizować rzeczywiste osiągnięcia Anonymous, którymi epatują nas media.

– *W światowej i polskiej prasie możemy przeczytać, że są wszędzie, rzucili Rosję na kolana, ukradli satelity szpiegowskie, ujawnili dane rosyjskich agentów z całego świata, przechwycili rosyjskie systemy łączności, zhakowali rosyjskie ministerstwo obrony* – zaczął swoje wystąpienie Łukasz Jachowicz.

Anonymous pod lupą

Łukasz Jachowicz wywodzi się ze środowiska aktywistów, przyglądał się więc efektom ataków Anonymous z przyjacielskim nastawieniem. Wszystko jednak wskazuje na to, że spektakularność tych działań w dużej mierze ma charakter medialny.

„Opanowanie Rosatomu" (nagłówek z polskiej prasy) polegało na utworzeniu nowej strony html z hasłem fckptn. Atak na stronę Roskosmosu to umieszczenie nowego wpisu. Po analizie 800 MB danych wykradzionych z rosyjskiego sektora kosmicznego okazało się, że to głównie skany uzgodnień dotyczące projektu lądownika czy sondy księżycowej – ktoś wykorzystał za szerokie uprawnienia do zasobów sieciowych i ściągnął archiwum. Rosyjska przestrzeń adresowa jest powszechnie skanowana i każdy otwarty dostęp do pdf jest natychmiast wykorzystywany.

Na to, że: „Rosja straciła dostęp do satelitów szpiegowskich" (kolejny tytuł prasowy) jedynym dowodem są cztery screenshoty z systemu zarządzania maszynami wirtualnymi. Były też szumne zapowiedzi ujawnienia listy tajnych agentów Kremla… i na razie cisza. – *Wygląda na to,*

że prasa podchwytuje ogłoszenia Anonymous, ale nikt tego nie weryfikuje – mówił Łukasz Jachowicz.

Z 10 GB, których wykradzenie z Nestle ogłoszono, Anonymous udostępnili zaledwie pięciomegabajtowe archiwum plików z baz danych (zamówienia, hasła, płatności, przedsiębiorstwa) zawierające wyłącznie losowe dane testowe. Po analizie losowych dokumentów z dużego wycieku danych z banku centralnego Rosji okazało się, że dotyczą archiwalnych kursów walut albo publicznych sprawozdań finansowych różnych firm. Nagłośnione ataki na stacje telewizyjne okazały się atakami na lokalne sieci kablowe. Uczciwie trzeba jednak przyznać, że pojawiają się także poważniejsze wycieki, typu 360 tys. plików z Roskomnadzoru (1TB).

Anonymous kreatywnie walczą z blokadą informacyjną w Rosji. Podmiana stron internetowych wielu mediów rosyjskich pozwoliła na przekazywanie prawdziwych informacji o inwazji. Przeprogramowano kilkaset kamer w ten sposób, że po wejściu do monitoringu pojawiały się treści, ujawniające skalę zbrodni dokonywanych przez Rosjan w Ukrainie. Inny sposób to dopisywanie komentarzy i dodawanie zdjęć tego, co się dzieje w Ukrainie, do różnych rosyjskich miejscówek: restauracji, muzeów, Kremla. – *Skanuje się rosyjską przestrzeń IT w poszukiwaniu otwartych, dostępnych drukarek i na nich drukuje się biuletyny informacyjne o wojnie w Ukrainie. Podejrzewam, że ktoś wpadnie na pomysł, że można wykorzystać technologię Chromecast i wkrótce na rosyjskich telewizorach podłączonych do Internetu pojawią się filmy z Ukrainy. Niedawno pojawiła się strona anonymous.xyz, na której publikowana jest część leaków brandowanych Anonymous, to ciekawe udogodnienie, będę te wycieki badał* – zapowiadał Łukasz Jachowicz.

Mamy też do czynienia z informacjami przypisywanymi Anonymous, ale się pod nimi ktoś konkretny podpisuje, np. białoruscy cyberpartyzanci – grupa sabotująca rodzimy transport, która nie chce, żeby przesyłano sprzęt wojskowy.

– *Zgadzam się , że wiele akcji Anonymous jest nieco przereklamowanych, ale zdarzają im się na prawdę spektakularne sukcesy. Ataki strony rosyjskiej również nie są imponujące, spodziewałem się wielu ataków zero-day, przejmowania infrastruktury obu krajów, a tego na razie nie widać* – podsumował spotkanie Rafał Chruściel.

amk

Przydatne źródła informacji:

- https://cert.gov.ua/articles
- https://www.rapid7.com/blog/post/2022/03/04/russia-ukraine-cybersecurity-updates
- https://fakenews.pl/

Skąd się wzięli Anonymous?

– *Dziennikarze piszą o grupie lub kolektywie hakerskim, sami Anonymous przed laty używali pojęcia internet gathering. To losowo dobierane grupki, które skrzykują się w interesującej ich sprawie i brandują się jako marka Anonymous. Pierwszy ich projekt, Chanology, był wyrazem walki ze scjentologią. Stali się rozpoznawalni po samobójstwie nastolatka Mitchella Hendersona, który zastrzelił się po utracie swojego iPoda, zajmowali się trollerką* – wyjaśniał Łukasz Jachowicz.

Stosunkowo łatwo uzyskać informacje o Anonymous w Internecie, całkiem pokaźnej strony dorobili się w Wikipedii, tutaj zasygnalizujemy więc tylko ważniejsze etapy działań tej formacji. W 2010 r. Anonymous przeprowadzili skoordynowaną grupę ataków – operację payback – skierowaną przeciwko wrogom piractwa internetowego. Przeszła ona płynnie w walkę z każdym, kto się sprzeciwiał ideom promowanym przez Wikileaks (na Visę, Mastercard, PayPala, które odcięły finansowanie WikiLeaks, przypuszczono ataki DDoS). Aktywność Anonymous zahaczyła o Polskę, w 2012 r. podczas trwania dyskusji o porozumieniu ACTA strona premier.gov.pl została podmieniona.

Od samego początku Anonymous stosowali klasyczne metody działania: ataki DDoS, podmienianie stron internetowych, wycieki danych (przypadkowe lub celowe), złośliwe telefony, czarne bomby, google bomby. Kontaktowali się głównie za pomocą usługi IRC. Udostępnili gorzej przygotowanym użytkownikom specjalne programy do przeprowadzania ataków DDoS przeciwko wskazanym przez Anonymous celom (najsłynniejszy z nich to Low Orbital Ion Cannon). Motywacje, jakie im przyświecały, to: zabawa, walka z cenzurą, walka z egzekwowaniem praw autorskich, walka o wolność, walka z nazistami.

– *Na podstawie informacji uzyskanych z kanału #OpRedScare widać, że po agresji na Ukrainę towarzystwo dobrze się bawi. Co chwila pojawiają się meldunki o kolejnych unieruchomionych systemach z domeny .ru – albo uruchamiano bootnety atakujące strony, albo przygotowano strony internetowe z javascript, które atakowały te serwisy. Na udostępnionej przez Rosjan liście adresów IP, z których uruchamiano ataki, jest kilkaset statycznych adresów z Polski. Nie było to ze strony naszych aktywistów najmądrzejsze, Rosjanie już o tym wiedzą* – mówił Łukasz Jachowicz.

Drony w natarciu

Nie ma chyba takiego drugiego środka bojowego, który w ciągu ostatnich kilkunastu lat zrobiłby większą karierę w wojsku niż drony. Kolejne konflikty, poczynając od walki z ISIS w Afganistanie czy Iraku, poprzez walki w Syrii, wojnę w Górnym Karabachu na Kaukazie czy teraz w Ukrainie pokazują, że ich skuteczne wykorzystanie nierzadko jest elementem przechylającym szalę zwycięstwa.

Jakie zalety decydują o tak wielkiej przydatności dronów podczas działań zbrojnych? Bezzałogowy statek powietrzny nie ma operatora na pokładzie, co w pierwszej kolejności niweluje ryzyko utraty życia pilota w przypadku katastrofy. Pozwala także zmniejszyć wielkość i masę statku powietrznego, a przez to wydłużyć czas i zasięg lotu. Cechy te sprawiają, że dron jest trudniej wykrywalny zarówno wizualnie, jak i radarowo, można z jego pomocą podejmować bardziej ryzykowne misje, bo jest także bardziej „cierpliwy" podczas obserwacji czy w oczekiwaniu na cel. Możliwość zabrania na pokład różnych sensorów i efektorów połączona z klasycznymi zaletami obserwacji z powietrza – z perspektywy lotu ptaka – decyduje o jego przydatności i otwiera nowe szanse dla użytkowników.

Karol Juszczyk

prezes Fundacji HiCenter, ekspert rynku i technologii systemów bezzałogowych. Współtwórca Polskiej Izby Systemów Bezzałogowych i Centrum Dronów w CNBOP PIB MSWIA. Współautor raportów dronowych Instytutu Mikromakro i podręczników dronowych dla samorządów, wieloletni członek jury konkursu akademickiego „Droniada".

Świadomość sytuacyjna

Współcześnie działania wojenne rozgrywają się w wielu domenach: lądowej, powietrznej, radiowej, informacyjnej czy cyberprzestrzeni. Zarówno sztab armii, jak i poszczególni żołnierze muszą podczas swoich działań uwzględniać jednocześnie wiele elementów pola walki: ostrzał artyleryjski, ataki z powietrza, ataki jednostek pancernych, specjalnych, zakłócenia łączności, dezinformację. W Ukrainie zanika klasyczny układ frontów, działania wrogich armii przenikają się

wzajemnie, prowadzenie skutecznych działań wojennych jest coraz bardziej skomplikowane i uzależnione od uwzględnienia coraz większej liczby elementów w tym samym czasie. Rosnący poziom złożoności wojny sprawia, że podstawą obrony staje się posiadanie odpowiedniej tzw. świadomości sytuacyjnej. Ilość, jakość i aktualność informacji decyduje o możliwości zapobiegania i zwalczania nadchodzących zagrożeń.

Możliwość zainstalowania na dronie różnych sensorów znakomicie predysponuje go do roli narzędzia poprawiającego świadomość sytuacyjną. Wyposażony w kamery światła widzialnego, kamery podczerwieni, czujniki laserowe może stanowić wsparcie jako element obserwacyjno-rozpoznawczy dla systemów artyleryjskich oraz dla lekkiej piechoty lub jednostek specjalnych.

Wsparcie dla artylerii

Agresor musi wykorzystywać ciężkie brygady zmechanizowane i pancerne jako taran niszczący opór wroga. Tego typu jednostki o dużej sile ognia oraz odporności balistycznej najlepiej niszczy z bezpiecznej odległości ciężka artyleria dużego kalibru. Dotychczas cele dla artylerii wskazywały wysunięte jednostki rozpoznawcze, co wiązało się z dużym ryzykiem dla żołnierzy. Obecnie tę rolę mogą spełniać drony. Drony operujące w bezpiecznej odległości dzięki kamerom o wysokiej rozdzielczości mogą skutecznie identyfikować odpowiednie cele do ataku, a za sprawą dalmierzy laserowych również udostępniać precyzyjne koordynaty celów czy wręcz bezpośrednio naprowadzać pociski kierowane i rakiety na cel. Kamery podczerwieni pozwalają na działania pod osłoną nocy, demolujące morale i siły witalne żołnierzy agresora.

W trwającym konflikcie ukraińską artylerią kierują m.in. polskie drony FlyEye, opracowane przez inżynierów należącej do WB Electronics gliwickiej spółki Flytronic.

Źródło: https://www.wbgroup.pl/app/uploads/2017/08/flyeye-34-scaled.jpg

FlyEye	
Wymiary	
Rozpiętość	3,6 m
Długość	1,8 m
Wysokość	0,43 m
Masa	
Startowa	do 12 kg
Osiągi	
Prędkość maksymalna	120 km/h
Prędkość minimalna	60 km/h
Pułap	5000 m n.p.m.
Zasięg	300 km (przy przemieszczającej się stacji naziemnej)
Długotrwałość lotu	2–4 h
Rozbieg	start z ręki

Wsparcie dla lekkiej piechoty i służb specjalnych

Lekkie i proste w użyciu drony konsumenckie okazały się doskonałym narzędziem wspierającym quasipartyzanckie działania zaczepno-nękające lekkiej piechoty, wyposażonej w ręczne zestawy przeciwpancerne. Drony służą z jednej strony do wyszukania kolumn pojazdów agresora, w szczególności podczas działań nocnych i z wykorzystaniem kamer podczerwieni, a z drugiej pomagają wybrać odpowiedni moment ataku podczas zawisu nad miejscem zasadzki podczas oczekiwania na przejazd wrogiej kolumny.

Wsparcie bezzałogowców okazuje się też być nieodzowne w czasie operacji specjalnych oraz na terenie miast. Miejskie kaniony uliczne są wręcz predysponowane do wykorzystywania dronów i znacząco przyczyniają się do wyłapywania grup dywersyjnych oraz kolumn lekkich pojazdów opancerzonych wojsk rozpoznawczych i specjalnych.

Drony to nie tylko sensory i poszerzanie świadomości sytuacyjnej. Furorę podczas walk w Ukrainie, a wcześniej w Górnym Karabachu, zrobiły drony produkcji tureckiej Bayraktar TB2. Drony te mogą nie tylko przekazywać dane obrazowe do operatora, lecz również wykonywać działania bojowe z wykorzystaniem ostrej amunicji. W Internecie możemy znaleźć wiele filmów świadczących o ich piekielnej skuteczności. Skąd się ona bierze?

Drony jako efektory

Przede wszystkim z nieprzeciętnych możliwości ukrycia swojej obecności. Wymiary TB2 (rozpiętość skrzydeł 12 metrów, długość 6,5 metrów) w połączeniu z pułapem praktycznym działania powyżej 5 kilometrów sprawiają, że dron ten jest

praktycznie niemożliwy do zaobserwowania gołym okiem i jest na poziomie gruntu niesłyszalny. Jego niska sygnatura radarowa oraz specyficzne protokoły łączności utrudniają również namierzenie go przez zestawy obrony przeciwlotniczej. Dodatkowo wykorzystywana amunicja to szybujące bomby nakierowywane laserowo. Brak sygnatury cieplnej oraz emisji hałasu tych pocisków daje dodatkową ochronę przed namierzeniem, a naprowadzanie laserem gwarantuje najwyższą precyzję uderzenia. Atak przychodzi „znikąd", bez żadnych sygnałów ostrzegawczych, co potęguje dezorientację wroga, szczególnie podczas działań nocnych.

Źródło: https://www.instalki.pl/images/newsy/03-2022/Bayraktar_TB2_ukraina.jpg

Bayraktar TB2	
Wymiary	
Rozpiętość	12 m
Długość	6,5 m
Masa	
Startowa	650 kg
Zapas paliwa	300 l
Osiągi	
Prędkość maksymalna	220 km/h
Prędkość przelotowa	130 km/h
Pułap	8200 m
Pułap praktyczny	5500 m
Zasięg	150 km
Długotrwałość lotu	27 h

Drony Bayraktar mogą zostać wyposażone tylko w maksymalnie cztery ładunki, więc ich bezcenna moc rażenia najczęściej jest wykorzystywana do ataków na tyłach kolumn wojskowych, gdzie niszczą: cenne transporty zaopatrzeniowe z amunicją i paliwem, pojazdy dowodzenia, mobilne stacje radarowe, zestawy obrony przeciwlotniczej oraz zestawy ciężkiej artylerii.

Wojska ukraińskie w coraz większym stopniu, stosownie do realizowanych dostaw, wykorzystują też tzw. amunicję krążącą profesjonalną, czyli niewielkie (około 1 metra rozpiętości) drony szybujące – płatowce potrafiące długo utrzymywać się w powietrzu i realizować działania obserwacyjne, a w przypadku namierzenia odpowiedniego celu spaść na niego w trybie „kamikadze" i zniszczyć ładunkiem znajdującym się na pokładzie. Obecnie Ukraina ma do dyspozycji amunicję krążącą produkcji polskiej (Warmate WB Elektronics) i amerykańskiej (Switchblade 300 i 600).

Wykorzystywane są też drony komercyjne wielowirnikowe do zrzucania na niewielkie odległości improwizowanych ładunków wybuchowych. Stosuje się do tego celu podwieszane ręczne granaty. Jest to broń bardzo skuteczna, w szczególności przeciwko piechocie, a jednocześnie jej zastosowanie jest niezwykle bezpieczne dla operatora.

Drony jako rejestratory

Drony podczas wojny w Ukrainie pełnią podwójną funkcję: umożliwiają realizację zadań bojowych, a jednocześnie pozwalają na rejestrację obrazów wojny. Filmy te mają duże znaczenie w walce informacyjnej, zagrzewają do walki i – rejestrując udane akcje zaczepne i obronne wojsk własnych – osłabiają morale wroga. Służą też do rejestracji przypadków łamania praw wojennych i dokumentowania zbrodni przeciw ludzkości. Te materiały mogą być dowodami w późniejszych postępowaniach przed sądami, podobnie jak rejestrowane zniszczenia wojenne obiektów cywilnych – w przyszłych postępowaniach odszkodowawczych czy reparacyjnych.

Systemy antydronowe

Jednym z ciekawszych zagadnień działań wojennych w Ukrainie jest niezwykła skuteczność wykorzystania bezzałogowców przez ukraińskich obrońców i porażka Rosjan na tym polu – to diametralnie inna sytuacja niż miała miejsce podczas aneksji Krymu w 2014 r.

Wydaje się, że są co najmniej dwie przyczyny tego stanu rzeczy. Prawdopodobnie strona ukraińska wypracowała wraz z zachodnimi sojusznikami dużo efektywniejsze metody i systemy obrony przed bezzałogowcami, bazujące na skutecznym ich wykrywaniu i neutralizowaniu za pomocą narzędzi walki elektronicznej. Tymczasem lata sankcji nałożonych na stronę rosyjską (np. na import podzespołów elektronicznych) zmusiły wojska rosyjskie do wykorzystywania w dużo większym stopniu mniej skutecznych systemów kinetycznych. Potwierdzają to materiały filmowe – relacje strony rosyjskiej dużo częściej pokazują kompletnie zniszczone (w wyniku eksplozji ładunku wybuchowego) drony ukraińskie, a na filmach strony przeciwnej często widzimy nieuszkodzone fizycznie, przechwycone elektronicznie drony rosyjskie.

Druga przyczyna to DNA obu armii i sposób prowadzenia działań wojennych. Prawdopodobnie strona rosyjska od

początku zakładała wykorzystanie takiego systemu zarządzania polem walki, w którym informacje pozyskiwane z rejonu walk są analizowane centralnie, centralnie również podejmowane są decyzje o działaniach poszczególnych grup batalionowych. Taki model jest zgodny z utrwalonym przez dekady w armii rosyjskiej systemem zarządzania oraz sposobami delegowania uprawnień i podejmowania decyzji. Gdy ten system nie zadziałał w pierwszych dniach agresji na Ukrainę, nie pojawiła się odpowiednia alternatywa ani dla zarządzania działaniami poszczególnych rodzajów wojsk, ani dla metod wykorzystania systemów bezzałogowych – stąd blamaż armii rosyjskiej w pierwszym miesiącu działań i niska skuteczność dronów po stronie rosyjskiej.

Obrońcy od początku postępowali inaczej. Jednostki działały w sposób rozproszony, ale na podstawie rozpoznania prowadzonego przez sojuszników przy jednoczesnym zachowaniu dużej autonomii w działaniu. Podejmowanie decyzji operacyjnych oraz wykorzystanie dronów na polu walki było dużo bardziej elastyczne, co zwiększyło szybkość reakcji na zmieniający się teatr wojenny. Okazało się, że demokratyczne mechanizmy w przeciwieństwie do centralnego zarządzania pozwoliły na lepsze wykorzystywanie potencjału dronów.

Operatorzy cywilni

Nie można też zapomnieć o ogromnym wsparciu dla wojsk ukraińskich – w szczególności gwardii narodowej – jakie jest nieustannie udzielane przez operatorów cywilnych bezzałogowych statków powietrznych. Osoby prywatne, w tym dziennikarze, wykorzystując posiadany komercyjny sprzęt, bardzo często wspomagają działania obronne – informują zawczasu o ruchach wojsk rosyjskich i umożliwiają szybką reakcję obrońców.

Niestety, sygnały nadawane przez stacje sterujące dronów cywilnych mogą być wykorzystywane do namierzania operatora i np. ostrzału artyleryjskiego. Po pierwsze, nieostrożne wykorzystywanie dronów komercyjnych może się skończyć śmiercią nie tylko operatora, lecz także osób postronnych, które mogą nawet nie być świadome wykorzystywania takiej aparatury w swoim otoczeniu. Po drugie, nie wiadomo jak w świetle Konwencji Genewskich traktować operatora: czy to cywil/dziennikarz dokumentujący zniszczenia wojenne, czy to już personel militarny, niepodlegający prawnej ochronie. Taka niejasna sytuacja prawna utrudnia pociągnięcie atakujących do odpowiedzialności karnej za ataki na cywilów.

Źródło: https://cdn.defence24.pl/2020/07/16/1920xpx/qdki3m-dronukrainasg.jpeg

Porównanie parametrów najpopularniejszych dronów komercyjnych			
	DJI MAVIC MINI	**DJI MAVIC AIR 2**	**DJI MAVIC 2**
Masa	249 g	570 g	Mavic 2 Pro: 907 g Mavic 2 Zoom: 905 g
Wymiary złożonego drona (dł. x szer. x wys.)	140×82×57 mm	180×97×84 mm	214×91×84 mm
Wymiary rozłożonego drona (dł. x szer. x wys.)	160×202×55 mm	183×253×77 mm	322×242×84 mm
GIMBAL I KAMERA			
Stabilizacja	3-osiowy gimbal	3-osiowy gimbal	3-osiowy gimbal
Rozdzielczość wideo	2.7 K: 2720×1530 25/30 p	4K Ultra HD: 3840×2160 24/25/30/60p 2.7K: 2720×1530 24/25/30/48/50/60p	Mavic 2 Zoom: 4K: 3840×2160 24/25/30p 2.7K: 2688×1512 24/25/30/48/50/60p Mavic 2 Pro: 4K: 3840×2160 24/25/30p 2.7K: 2688x1512 24/25/30/48/50/60p
Sensor	1/2,3" CMOS	1/2" CMOS	Mavic 2 Zoom: 1/2.3" CMOS Mavic 2 Pro: 1" CMOS
Piksele	12 MP	48 MP	Mavic Piksele: 12 MP Mavic Piksele: 20 MP
Format zdjęć	JPEG, MP4	JPEG, DNG RAW, MP4, MOV	JPEG, DNG RAW, MP4, MOV

KONTYNUACJA

OSIĄGI PODCZAS LOTU			
Maksymalny czas lotu	30 minut (w bezwietrznych warunkach)	34 minuty (w bezwietrznych warunkach)	31 minut (w bezwietrznych warunkach)
Maksymalna akceptowalna siła wiatru	28,8 km/h	29–38 km/h	29–38 km/h
Maksymalna prędkość (na wysokości ok. poziomu morza przy bezwietrznych warunkach)	46,8 km/h (tryb sportowy)	68,4 km/h (tryb sportowy)	72 km/h (tryb sportowy)
Zasięg	do 4 km	do 10 km	do 8 km
System transmisji obrazu	ulepszone Wi-Fi	OcuSync 2.0	OcuSync 2.0
Temperatura operacyjna	0°C–40°C	-10°C –40°C	-10°C–40°C
System omijania przeszkód	Brak systemu omijania przeszkód.	System omijania przeszkód z czujnikami z przodu, z dołu oraz z tyłu drona.	System omijania przeszkód z czujnikami na całej powierzchni drona: z przodu, z tyłu, z dołu, z góry oraz z obu boków drona.
Inteligentne tryby lotu	Return-to-Home (powrót do bazy), CineMode, tryby QuickShot: Dronie, Circle, Helix, Rocket	ActiveTrack 3.0, Spotlight 2.0, POI 3.0, Tripod, Hyperlapse 8K, tryby QuickShot: Circle, Helix, Dronie, Rocket, Asteroid, Boomerang	ActiveTrack 2.0, Hyperlapse, Point of Interest, Waypoints, Cinematic Mode, TapFly, tryby QuickShot: Circle, Helix, Dronie, Rocket, Asteroid, Boomerang

Niewątpliwie bezzałogowe statki powietrzne podczas wojny w Ukrainie w skuteczny sposób zniwelowały część przewag, którymi dysponowały wojska rosyjskie, zwłaszcza w środkach lotniczych. Nie narażano przy tym personelu obsługi – katastrofa drona nie oznacza konieczności uzupełnienia, przeszkolenia nowego operatora, co niestety często ma miejsce w przypadku pilotów statków załogowych po zestrzeleniu. Ponadto drony są od kilkunastu do kilkudziesięciu razy tańsze i w zakupie, i w eksploatacji. Przy istotnej różnicy potencjałów ekonomicznych obydwu walczących państw ma to niebagatelne znaczenie. Drony wzmocniły możliwości eliminacji systemów przeciwdostępowych przeciwnika. Ich wysoka skuteczność w niszczeniu tych instalacji jest opłacalna nawet przy dużych stratach własnych – drony z reguły są dużo tańsze niż eliminowane przez nie systemy obrony przeciwlotniczej.

Przyszłość: autonomiczne roje dronów

Przykład udanego wykorzystania dronów przez potencjalnie słabszą militarnie stronę w Ukrainie jeszcze bardziej przyśpieszy ich rozwój. Należy się spodziewać coraz szerszego wykorzystywania dronów na współczesnym polu walki, w tym całych grup dronów – tzw. rojów dronów. Przy wzrastającej liczbie dronów kluczowe będzie wdrożenie technologii pozwalających na ich autonomiczne działanie i szerokie wykorzystanie systemów wspomagania decyzji z wykorzystaniem sztucznej inteligencji. Ilość gromadzonych danych (w szczególności danych obrazowych) przez rój dronów podczas pojedynczej misji będzie tak ogromna, że zacznie przekraczać nie tylko dzisiejsze możliwości analityczne operatora, lecz także przepustowości systemów łączności. Dlatego dron przyszłości będzie „mądrzejszy" i bardziej „samodzielny".

Technologie dronowe, robotyczne, autonomiczne, sztucznej inteligencji – to obszar tematyczny będący w centrum zainteresowań ośrodka badawczo-rozwojowego Poznańskiego Centrum Superkomputerowo-Sieciowego, powstającego na lotnisku w Kąkolewie pod Poznaniem. Obecnie zadania badawcze są skumulowane w trzech głównych, innowacyjnych obszarach badawczych:

- eksploatacja BSP/ZSP (bezzałogowy/załogowy statek powietrzny);
- obszary zastosowania BSP/ZSP;
- eksploatacji lotnisk: integracja rozwiązań w systemie zarządzania lotniskiem, w tym elementów infrastruktury, bezpieczeństwo i ochrona funkcjonowania lotniska.

Nowoczesna baza laboratoryjna obejmować będzie m.in.:

- Laboratorium Autonomicznej i Energooszczędnej Infrastruktury Lotniska,
- Laboratorium Bezpieczeństwa i Ochrony Eksploatacji Lotniska,
- Laboratorium Rozwoju Bezzałogowych Statków Powietrznych,
- Laboratorium Rozwoju Systemów Kontroli Lotów i Przestrzeni Powietrznej.

Właśnie na lotnisku w Kąkolewie i na targach ITM MTP w Poznaniu na przełomie maja i czerwca br. odbędzie się DronePower Hackathon. Więcej informacji na stronach: DronePower.pl i aerospacelab.psnc.pl

Rosja reaguje na sankcje IT

Wśród sankcji uruchomionych przeciwko Rosji najbardziej nagłośniono problem surowców energetycznych i wykluczenie rosyjskich banków z systemu SWIFT. Dużo czytamy o elektryzującym bogatych Rosjan zakazie importu brylantów i ekskluzywnych zegarków, i o ważnym dla maluczkich zamknięciu McDonalda. Trochę umyka nam fakt, że Rosja utraciła zdolność do produkowania dóbr technologicznych. Jak dotkliwe dla Rosji będą sankcje IT? Doniesienia mediów rosyjskich (m.in. „Prawdy", „Komsolskiej Prawdy", Gaziety, „Kommiersanta") skonfrontowaliśmy z doniesieniami światowymi.

Ludzie są podatni na zniekształcenia percepcyjne i zawsze lubią rzeczy, które potwierdzają ich punkt widzenia. Mamy jakiś pogląd na stan rzeczy i gdy czytamy to samo w sieci społecznościowej, myślimy, schlebiając sobie: *fajnie, ja to wiedziałem!* Tak działają internetowe media społecznościowe, algorytmicznie dostosowując się do naszych preferencji, a my żyjemy w tej pięknej, własnej, przytulnej bańce informacyjnej.

Stare media działają podobnie. Ludzie czytają gazety i oglądają kanały TV, których treści odpowiadają ich poglądom. Sieci społecznościowe odtworzyły ten model. Wcześniej szansą na wydostanie się z bańki były intensywniejsze bezpośrednie relacje, teraz wszystko jest online. Jesteśmy stale manipulowani przez wysokiej klasy specjalistów i trudno się przed tym obronić. Gdy w Finlandii w 2015 r. nasiliły się działania rosyjskich trolli, prezydent Sauli Niinistö wezwał Finów do wzięcia odpowiedzialności za walkę z fake newsami. Do Helsinek dotarli amerykańscy eksperci, którzy

Zbigniew Daleczko

matematyk po Uniwersytecie Wrocławskim, specjalizujący się w teorii liczb, autor systemu operacyjnego i języka programowania „KB" na minikomputer MERA-100. Rzeczoznawca Polskiego Towarzystwa Informatycznego.

doradzali urzędnikom, jak rozpoznać fałszywe wiadomości, zrozumieć, dlaczego są one rozpowszechniane i opracować strategie walki z nimi. Zreformowano również system edukacji, kładąc nacisk na krytyczne myślenie, tak żeby już od najmłodszych lat uczyć prawidłowego podejścia do oceny wiadomości. – *To nie jest tylko problem rządu – celem ataków jest całe społeczeństwo. Robimy, co do nas należy, ale ochrona fińskiej demokracji jest zadaniem każdego z nas. Pierwszą linią obrony jest nauczyciel w przedszkolu* – powiedział wówczas CNN Jussi Toivanen, główny specjalista ds. komunikacji fińskiego premiera.

Rosyjska narracja

Rosja jest największym krajem na świecie. Ma niezwyciężoną, drugą co do wielkości armię na świecie posiadającą broń jądrową i kosmiczną. Rosję popiera większość krajów wolnego świata, wliczając to najludniejszy kraj świata Chiny, Indie, Afrykę, Amerykę Łacińską, kraje arabskie... Rosja ma wszystkie potrzebne światu minerały, złoto, diamenty, a przede wszystkim źródła energii, takie jak węgiel, gaz, ropa naftowa od których uzależniona jest niewielka Gej-ropa. Rosja to potęga techniczna i technologiczna z zaawansowaną techniką kosmiczną i zbrojeniową. Mamy demokratycznie wybranego Prezydenta i demokratyczne rządy, ale mamy też wroga Stany Zjednoczone, które straciły swoją rolę na świecie i starają się ją odzyskać, atakując Rosję za pomocą sojuszu NATO i wykorzystując do tego europejskie kraje. Dlatego musimy się bronić, by odzyskać dawną potęgę – robi to Putin, a wspiera go głowa prawosławia patriarcha Cyryl.

Tak w wielkim skrócie wygląda kluczowy dla Kremla przekaz propagandowy kierowany do wewnątrz kraju. Realizowany jest poprzez zmasowane działania propagandowe (akcje poparcia litery Z), ograniczanie wolności słowa, wyłączenie sieci społecznościowych, a także wysiłki na rzecz odłączenia Rosji od sieci globalnego Internetu i wprowadzenie własnego Runetu, analogicznie do modelu chińskiego.

Ten przekaz propagandowy nie jest jednak szczelny i postanowiliśmy przyjrzeć się rosyjskiej bańce informacyjnej, żeby zdiagnozować sygnalizowane już tam problemy związane z sankcjami w obszarze IT.

Powtórka z CoComu?

W odwecie za agresję militarną na Ukrainę Rosja została objęta bardzo poważnymi sankcjami. Obejmują one także wstrzymanie dostaw rozwiązań informatycznych. W lutym i marcu br. wiele globalnych firm informatycznych (Microsoft, IBM, Dell, Cisco, Asus, AMD i Intel) ogłosiło wycofanie się z rynku rosyjskiego. Także Taiwan Semiconductor Manufacturing wprowadza sankcje, co przeszkodzi w produkcji chipów Elbrus, które Rosja wykorzystuje militarnie.

Mimo wysiłków Rosja nie dorobiła się jeszcze własnego przemysłu półprzewodnikowego, a dotychczasowe próby na tym polu nie napawają optymizmem. Procesor Baikal-S wprawdzie działa, ale do jego masowych zastosowań droga daleka, testy Elbrus-8C wypadły kiepsko i te procesory nie wszędzie mogą być stosowane. Przyjmując optymistyczne założenia, dopiero za kilka lat – i to przy istotnym wsparciu państwa i dużego krajowego biznesu, zwłaszcza w partnerstwie z innymi krajami (na przykład BRICS) – Rosja będzie w stanie uruchomić własną produkcję mikroelektroniki zgodną ze standardami technologicznymi 28 lub 14 nanometrów.

Brak nowoczesnych procesorów niewątpliwie dotkliwie wpłynie na wiele sektorów gospodarczych Rosji. Przy obecnej skali cyfryzacji w gospodarce i działaniach rządu, serwery i systemy pamięci masowej są dziś wykorzystywane absolutnie wszędzie – z rosyjskim sektorem wojskowym na czele. Mamy więc poniekąd przedsmak układu CoCom, który przed laty zablokował państwom bloku wschodniego dostęp do nowoczesnych technologii, co wpędziło ZSRR i jego projekty kosmiczne w poważny rozwojowy impas. Teraz skutki jednak nie muszą być równie dotkliwe, zważywszy na chińskiego sojusznika Rosji.

Motoryzacja w opałach

Rosyjskie fabryki samochodów szukają sposobów na import komponentów i przygotowują się do znacznego uproszczenia konfiguracji produkowanych samochodów. Najtrudniej jest to zrobić w przypadku elektroniki i skomplikowanych podzespołów – znalezienie alternatywnych dostawców i wprowadzenie ich wyrobów do produkcji może wymagać nawet roku czasu. Sankcje i przerwy w łańcuchach dostaw powodują, że nawet rodzime marki samochodów intensywnie poszukują zamienników swoich zwykłych komponentów. Tak więc przykładowo AvtoVAZ zapowiedział specjalne wersje Łady, w których niektóre krytycznie ważne importowane komponenty zostaną zastąpione alternatywnymi rozwiązaniami. Uproszczenia mogą dotyczyć przede wszystkim elektroniki, w tym aktywnych systemów bezpieczeństwa, czujników parkowania, multimediów, klimatyzacji. Możliwe jest również uproszczenie układu paliwowego.

> *Gazeta.ru zwróciła się do rzecznika Ministerstwa Przemysłu i Handlu z pytaniami o to, czy rosyjscy producenci samochodów uzyskają prawo do produkcji samochodów bez hamulców, stabilizacji kursu i poduszek powietrznych oraz o plany zmniejszenia wymagań środowiskowych dla samochodów.... Ministerstwo odmówiło komentarza.*

Nie ma jednak pewności, czy kontrolujący AvtoVAZ koncern Renault pozwoli na instalację komponentów pochodzących spoza zatwierdzonej puli dostawców.

Rosyjskim dealerom samochodowym wyczerpały się już oryginalne części zamienne i materiały eksploatacyjne. Nie można zdobyć części dla wielu marek: Volkswagena, Skody i Porsche, BMW, Mercedes-Benz, Jeepa i Mazdy. Sytuacja jest znacznie bardziej skomplikowana w przypadku dużych, technologicznie skomplikowanych jednostek, które z reguły można kupić tylko u oficjalnych dealerów samochodowych – np. nie jest już dostępna jednostka mechatroniki (jednostki elektrohydraulicznej w automatyce) do crossovera BMW X1.

KamAZ też nie będzie w stanie wyprodukować sprzętu wojskowego, bo wyposażył ciężkie pojazdy o nośności ponad 20 ton tylko w niemieckie 16-biegowe skrzynie ZF16. Teraz KamAZ będzie musiał ograniczyć montaż wielu modeli, w tym podwozia 63501, które służyło do montażu różnych wojskowych pojazdów specjalnych. Produkcja ośmiokołowego podwozia 6560, które jest podstawą dla systemu obrony przeciwlotniczej Pantsir, również będzie wstrzymana, a armia rosyjska pozostanie bez ciągnika czołgowego 6522.

Ofensywa amerykańska

Stany Zjednoczone w ramach sankcji podjęły też działania pozbawiające Moskwę możliwości zakupu zagranicznych części do rosyjskiego sprzętu wojskowego. Waszyngton zapowiada, że będzie celował w kluczowe węzły w łańcuchach dostaw, aby osłabić rosyjskie wojsko i przemysł obronny, który nadal opiera się na zachodniej technologii. W marcu br. Departament Handlu USA wprowadził nowe środki kontroli eksportu, aby uniemożliwić Rosji dostęp do półprzewodników, telekomunikacji, sprzętu bezpieczeństwa informacji, laserów i czujników zawierających technologię amerykańską – nawet jeśli zostały wyprodukowane poza Stanami Zjednoczonymi.

Jednocześnie Senat USA większością głosów uchwalił ustawę mającą na celu poprawę konkurencyjności gospodarki amerykańskiej. Przewiduje zmniejszenie zależności od dostaw kluczowych rodzajów komponentów (w szczególności chipów i sprzętu telekomunikacyjnego), zwiększenie konkurencji z chińskimi firmami z sektora high-tech, a także dodatkowe środki ochrony rynku amerykańskiego. Aby pobudzić produkcję chipów w Stanach Zjednoczonych, ustawodawcy chcą wydać 52 mld dolarów. Amerykańska ustawa o konkurencyjności (America Competes Act) przewiduje redukcję zależności od zagranicznych technologii i zapewnienie samowystarczalności zaopatrzenia USA.

Systemy WRE

Systemy walki radioelektronicznej WRE były uważane za rosyjską specjalność. Rosja rozwijała ich wiele i o różnym przeznaczeniu – od utrudniania pracy radarów przeciwnika, poprzez maskowanie własnych emisji elektromagnetycznych, niszczenie nadlatujących, sterowanych radiowo pocisków, po zakłócanie łączności komórkowej czy systemu GPS. Rosja z powodzeniem testowała działanie takich rozwiązań podczas walk w Donbasie w 2014 r. Strona ukraińska była wówczas bezbronna wobec takich rosyjskich systemów WRE, jak Rtuć-BM czy Krasucha-4 .

Brak chipów stał się jedną z kluczowych przeszkód w zwiększaniu wielkości produkcji na świecie po usunięciu ograniczeń związanych z koronawirusem. Dotknęło to wielu branż – od elektroniki po motoryzację. Tajwańska firma TSMC odpowiada obecnie za ponad połowę produkcji chipów (54 proc. udziału w rynku), następny jest Samsung (17 proc.) i tajwańska UMC (7 proc). W sumie firmy południowokoreańskie (18 proc.) i tajwańskie (63 proc.) produkują 87 proc. chipów na świecie (mowa tu o łącznej fizycznej produkcji chipów, w tym układów zaprojektowanych przez deweloperów z innych krajów, dla których chipy montowane są w tych samych głównych fabrykach), a największy chiński producent chipów SMIC jest na czarnej liście w USA.

Obecna odsłona wojny w Ukrainie zmieniła ten obraz. Rosjanie wydają się bezradni – ich łączność nie działa, radary nie wykrywają zagrożenia, a oddziały gubią się w terenie. Ważni oficerowie giną ściągając na siebie ogień po rozmowach przez zwykłe, łatwe do podsłuchania i namierzenia telefony komórkowe, będące dla Ukraińców oznaczeniem celu.

Luzowanie przepisów

Jednocześnie Rosji grozi kolejna runda sankcji, ostrzejszych niż kiedykolwiek wcześniej. Ambasador Rosji w USA Anatolij Antonow nazwał nowe amerykańskie sankcje nałożone na rosyjski sektor technologiczny nielegalnymi, mówiąc o celowych próbach ograniczenia technologicznego rozwoju jego kraju. Aby wesprzeć nadwątloną sankcjami gospodarkę, rząd zamierza dokonać zmian w systemie zamówień publicznych – część z nich została już uchwalona przez Dumę Państwową. Rząd, władze regionalne i gminy będą miały prawo do zmiany warunków zawartych w kontraktach państwowych, dopuszczono również rozszerzenie możliwości zakupów od jednego dostawcy. Rosyjski resort cyfryzacji chce także ułatwić import komponentów poprzez uproszczenie procedur i wprowadzenie zerowych stawek celnych. W połowie marca br. powstał plan działań priorytetowych, zapewniających

rozwój rosyjskiej gospodarki w obliczu presji sankcji zewnętrznych – władze rozważają możliwość wskazania skonsolidowanego kontrahenta na zakup sprzętu komputerowego i telekomunikacyjnego.

Co więcej, Ministerstwo Cyfryzacji przygotowało projekt ustawy, która ma ułatwić firmom IT dostęp do zamówień rządowych. Planowane jest także ograniczenie odpowiedzialności dostawców za niepełne wykonanie zamówienia oraz ograniczenie dostępu do informacji o zamówieniach.

Do końca 2022 r. liczba miejsc pracy w rosyjskiej gospodarce może zostać zmniejszona o 2 mln, przez co stopa bezrobocia w kraju wzrośnie z obecnych 4,4 proc. do 7,1–7,8 proc. Spadek liczby miejsc pracy nastąpi przede wszystkim w branżach uzależnionych od importowanych komponentów (przemysł motoryzacyjny, AGD), jak i w tych, które utraciły zewnętrzne (hutnictwo, produkcja nawozów) lub krajowe (budownictwo) rynki zbytu na skutek sankcji. Są to branże, w których mamy do czynienia z odejściem głównych kontrahentów, wzrostem kosztów produktów importowanych ze względu na dewaluację rubla lub ze skutkami sankcji – część dostaw zagranicznych została wstrzymana z powodu sankcji (mikroelektronika, telekomunikacja).

Exodus programistów

Po rozpoczęciu inwazji z Rosji wyjechało około 70 tys. informatyków, najczęściej do Gruzji, Kazachstanu, Armenii czy krajów, które zwlekały z sankcjami. Wielu z tych specjalistów wyląduje zapewne w UE lub USA, choć nie jest to takie pewne z uwagi na specyfikę branży wymagającej wzajemnego zaufania dostawcy i klienta. Rosyjskie Stowarzyszenie Komunikacji Elektronicznej przewiduje, że w następnej, kwietniowej fali kraj opuści kolejne 70–100 tys. informatyków. Sankcje, jakimi obłożona jest Rosja, nie ułatwiają podróżowania, a rosyjski paszport na świecie dziś bardziej przeszkadza niż pomaga, ale masowa ucieczka pracowników IT do innych krajów będzie trudna do zatrzymania.

Rosyjska Duma próbuje mamić specjalistów specjalnymi programami. Mowa tu o trzyletnim zwolnieniu z podatków dla firm informatycznych, preferencjach podatkowych dla firm wdrażających rozwiązania techniczne i odroczeniu powołania do wojska dla programistów. Te działania – ze względu na duży spadek wartości rubla, trudności z wypłacalnością wynagrodzenia czy zamknięcie działalności firm zachodnich – raczej pracowników sfery IT przed ucieczką nie powstrzymają. Pojawiają się jednak – na razie dementowane przez władzę – doniesienia, że osoby o wykształceniu informatycznym nie będą wypuszczane z Rosji.

Rosyjscy programiści mają renomę – są świetnie wykształceni, bo bogate tradycje matematyczne w Rosji przekładają się na wysoki poziom nauczania, także informatyki. Biegle posługują się angielskim, cenią sobie zglobalizowany świat, to nie jest elektorat, który kupowałby brednie Putina o denazyfikacji. Nie będzie więc łatwo zastąpić wysoko wykwalifikowanych specjalistów w wielu gałęziach gospodarki rosyjskiej.

Premier Michaił Miszustin podpisał nowy dekret o wcieleniu do wojska, opublikowany w oficjalnym rządowym kanale. Dekret rozszerza odroczenie z wojska na informatyków w wieku poborowym, pod warunkiem posiadania wyższego wykształcenia i rocznego stażu pracy. Lista specjalizacji, które ten dekret obejmie, zostanie opracowana przez firmy informatyczne i po zatwierdzeniu przez Ministerstwo Cyfryzacji i przesłana do wojskowych urzędów rejestracji i rekrutacji oraz Ministerstwa Obrony.

W ramach wsparcia dla branży rosyjscy informatycy zostaną zwolnieni z płacenia podatku dochodowego i kontroli organów regulacyjnych. Będą też mogli zaciągnąć specjalne kredyty o oprocentowaniu nieprzekraczającym 3 proc. Dodatkowo informatycy w wieku od 22 do 40 lat będą mogli ubiegać się o preferencyjne kredyty hipoteczne.

Software'owy patriotyzm

Putin zabronił agendom rządowym kupowania i używania zagranicznego oprogramowania – w ciągu miesiąca rząd ma opracować i zatwierdzić wymagania dla oprogramowania używanego przez organy państwowe i agendy rządowe oraz zatwierdzić zasady jego zakupu.

Podpisany przez Putina dekret o niezależności technologicznej Rosji wprowadził zakaz zakupu zagranicznego oprogramowania dla obiektów informacyjnej infrastruktury kry-

tycznej Rosji od 31 marca br. Ponadto od 1 stycznia 2025 r. władze państwowe będą miały zakaz używania obcego oprogramowania w takich obiektach bez zgody uprawnionego organu wykonawczego. Zamawianie usług wymaganych do korzystania z obcego oprogramowania w tych obiektach jest możliwe tylko po uzgodnieniu z federalnym organem wykonawczym, upoważnionym przez rząd Federacji Rosyjskiej.

Agencje rządowe w Federacji Rosyjskiej używały zachodniego oprogramowania od dziesięcioleci, praca na starych programach jest nadal dozwolona.

Rodzimy open source

Microsoft jest monopolistą na rosyjskim rynku systemów operacyjnych i oprogramowania biurowego i opanował, według Federalnej Służby Antymonopolowej (dane z początku 2019 r.), ponad 95 proc. systemów operacyjnych rynku, a według różnych źródeł – od 74 do 90 proc. rynku oprogramowania biurowego.

Własne oprogramowanie open source Rosja rozwija dopiero od 20 lat. Kilka lat temu przy zamówieniach rządowych zarekomendowano rodzimy system operacyjny AlterOS (firmy Almi Partner), bazujący na jądrze Linux i łączący zalety różnych systemów operacyjnych. Zaletą AlterOffice jest intuicyjny interfejs, a podobieństwo funkcjonalne do znanego wszystkim pakietu Microsoft Office sprawia, że przejście od oprogramowania importowanego do rodzimego jest bardzo wygodne. Serwery repozytoriów znajdują się w Rosji, serwerownie są wyposażone zgodnie z wymogami FSTEC (Federalnej Służby Kontroli Technicznej i Eksportu) i są chronione przed nieautoryzowanym dostępem. Z tego oprogramowania od 2017 r. korzystają: Ministerstwo Sytuacji Nadzwyczajnych, Ministerstwo Pracy, Ministerstwo Sprawiedliwości, Ministerstwo Rozwoju Gospodarczego, Duma Państwowa Federacji Rosyjskiej, a także wiele administracji regionalnych i ministerstw.

Open source wydaje się dla Rosji jedyną szansą na częściowe zastąpienie importu oprogramowania, a tym samym złagodzenie skutków sankcji, choć może to być droga wyboista. Ataki hakerskie, zintensyfikowane po inwazji Rosji na Ukrainę, nie omijają tego oprogramowania, w ciągu jednego tygodnia obejmującego przełom marca i kwietnia br. rosyjscy programiści zarejestrowali ponad 30 przypadków wprowadzenia szkodliwego kodu do produktów open source.

Valery Andreev, zastępca dyrektora generalnego ds. nauki i rozwoju w firmie IVK, uważa, że takie incydenty powinny być kolejnym powodem utworzenia przez Rosję krajowego repozytorium open source. Ponieważ moduły open source są publikowane wraz z kodem źródłowym, można je sprawdzić pod kątem złośliwych funkcji przed integracją z produktem, ale w tym celu niezbędne jest rozwiązanie systemowe analizy kodów źródłowych w trybie ręcznym i automatycznym, co wymaga opracowania odpowiednich narzędzi.

Problemów jest wiele, nie bardzo na przykład wiadomo, czym zastąpić oprogramowanie do zarządzania dużymi przedsiębiorstwami typu SAP. Będziemy pilnie śledzić próby wybijania się Rosji na technologiczną niepodległość.

Sieci się posypią

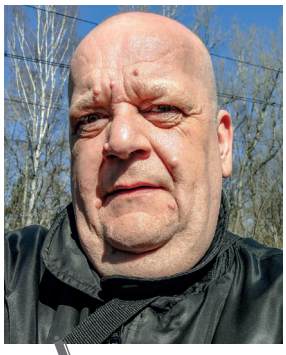
21 marca br. obradował Rosyjski Związek Przemysłowców i Przedsiębiorców (RSPP) ds. komunikacji i IT (w jego skład wchodzą przedstawiciele MTS, MegaFon, VimpelCom, ER-Telecom, GS Group, Kolei Rosyjskich i innych firm) w sprawie działań zapewniających rozwój telekomunikacji i technologi informacyjno-komunikacyjnych w warunkach presji sankcji zewnętrznych. Jak donosi „Kommiersant", z dokumentu przygotowanego po posiedzeniu wynika, że koszt sprzętu telekomunikacyjnego wzrósł już o 40 proc. z powodu odejścia zachodnich dostawców i deprecjacji rubla, a może wzrosnąć o kolejne 80 proc. W obecnych warunkach ekonomicznych rezerwy sprzętowe operatorów telekomunikacyjnych wystarczą na zapewnienie funkcjonowania infrastruktury przez cztery do sześciu miesięcy. Tym samym od lipca wzrośnie ryzyko wypadków i zakłócenia stabilności sieci. Dotyczy to również sieci komunikacyjnych transportu kolejowego i kompleksu paliwowo-energetycznego. – *Jedynym sposobem na utrzymanie działającej infrastruktury jest ograniczenie wszelkich planów rozwojowych i wykorzystanie zakupionego wcześniej sprzętu wyłącznie w celu utrzymania stabilności sieci* – zaleca RSPP.

Rosyjscy specjaliści ostrzegają, że będą również problemy z zasięgiem Internetu. Nieograniczony dostęp do Internetu powoduje poważne obciążenie sieci, sprzęt zużywa się bardziej, a podzespoły do stacji bazowych są już niedostępne. Wg „Komsomolskiej Prawdy" MinTsifry zaapelował o eksploatację sprzętu w trybie oszczędzania, co operatorzy telekomunikacyjni popierają. Ddotychczasowe taryfy z nielimitowanym Internetem zostaną w ciągu kilku miesięcy przeniesione do „limitowanych" pakietów – najprawdopodobniej operatorzy zaoferują pakiet internetowy 50 GB zamiast nieograniczonego.

Nie dajmy się skopać Pegazowi

Nie ma przesady w stwierdzeniu, że ostatnie 30 lat rozwoju techniki to dzieje ogołacania człowieka z prywatności przez urządzenia IT. Z każdym rokiem przybywało bowiem problemów dotyczących bezpieczeństwa danych, a jednocześnie coraz więcej danych odnosiło się do naszego życia prywatnego.

Tomasz Kulisiewicz
sekretarz Sektorowej Rady ds. Kompetencji – Informatyka



Jacek Grabowski
wieloletni dziennikarz prasy komputerowej

W pamięci komputerów z czasem zaczęliśmy gromadzić prywatne zdjęcia i notatki, badania lekarskie, dowody płatności i wpływów na nasze konto oraz wiele innych dokumentów, pozwalających precyzyjnie odtworzyć wszystkie nasze czynności, prześledzić znajomości, hobby, czy te najbardziej skryte preferencje seksualne. Obecnie najwięcej takich wrażliwych danych mieści się oczywiście w smartfonie.

Specjaliści od bezpieczeństwa informatycznego mówią półżartem, że jesteśmy tyle warci, ile są warte nasze dane. Z punktu widzenia policji „tajnych, widnych i dwupłciowych" aktywność większości ludzi nie jest warta angażowania sił w zdobywanie zawartości pamięci ich smartfonów. Ale, jak wiemy, przypadki podsłuchiwania zdarzają się – i są coraz częstsze. Dlatego też hasło „Pegasus" coraz śmielej przebija się na nagłówki gazet i paski informacyjne. Niemal otoczone legendą oprogramowanie szpiegujące, opracowane przez izraelską firmę NSO Group, miało być wykorzystywane do śledzenia opozycji, ataki tego systemu na swoje telefony rzekomo odnotowali też funkcjonariusze NIK.

Miłe złego początki

Sławny Kevin Mitnick, dwukrotnie skazany w latach 90. za włamania do systemów komputerowych (na wymiar drugiego wyroku wpływ miało fałszywe oskarżenie, że używając gwizdka naśladującego wybieranie tonowe może się włamać do systemu NORAD i wywołać wojnę nuklearną), późniejszy konsultant do spraw cyberbezpieczeństwa i współwłaściciel specjalistycznych firm, w których pełni m.in. funkcję Chief Hacking Officer, włamywał się do systemów komputerowych i central poprzez linie telefonii stacjonarnej. Klonowanych komórek używał tylko dla zacierania swoich śladów włamań.

Według artykułu opublikowanego przez Kaspersky Lab w 2014 r. pierwszym wirusem na telefony komórkowe (a ściślej – robakiem, bo był samoreplikujący i nie potrzebował, jak wirusy, nośnika w postaci zainfekowanego pliku wykonywalnego) był Cabir, zwany też SymbOS/Cabir, Symbian/Cabir i EPOC.cabir, który pojawił się w 2004 r., atakując ówczesną nowość – telefony Nokii z procesorami ARM, pracujące pod kontrolą systemu SymbianOS (Nokia 7650, Nokia 3650, Nokia Communicator 9000 i kolejne). Cabir był raczej ćwiczeniem grupy prezentującej się jako A29, która chciała wskazać na zagrożenia – nie umożliwiał kradzieży danych, nie szyfrował pamięci ani nie kasował jej zawartości. Jedynymi widomymi efektami były napis Cabir pojawiający się na wyświetlaczu po włączeniu telefonu oraz rozładowanie baterii w ciągu 2–3 godzin, co wtedy było bardzo zaskakujące, bo np. niezapomniana Nokia 6310i (z systemem NokiaOS i Javą) działała nawet przez 6 godzin nieprzerwanej rozmowy i wymagała ładowania dopiero po 17 dniach czuwania. Szybkie rozładowywanie zaatakowanego telefonu powodowane było tym, że Cabir nieustannie przeszukiwał otoczenie, by móc przeskakiwać na pobliskie telefony, korzystając z transmisji Bluetooth. Jego wersja zwana Mabir potrafiła się upowszechniać także poprzez MMS-y. SymbianOs został jednak uszczelniony, a w 2012 r. Nokia z niego zrezygnowała, więc twórcy wirusów szybko przestawili się na dużo bardziej „przydatne" dla nich malware na Javę. W latach 2009–2010 pojawiły się trojany i botnety działające w środowisku Androida i iOS. Ich działanie nie ograniczało się tylko np. do wysyłania bez wiedzy użytkownika spamowych SMS-ów czy SMS-ów na płatne numery. Zaczęło się przejmowanie telefonów użytkowników w celach zdecydowanie przestępczych, a wraz z rozwojem bankowości mobilnej – przechwytywanie i przekierowywanie dostępu do kont bankowych. W 2012 r. malware znalazło się nawet w App Store i Android Market (jak wtedy nazywał się Google Play).

Antenaci Pegasusa

W 2009 r. w sieci jednego z operatorów Zjednoczonych Emiratów Arabskich rozesłany został SMS z linkiem dla klientów biznesowych smartfonów BlackBerry. Rzekoma aktualizacja bezpieczeństwa instalowała na nich oprogramowanie szpiegujące.

Już w 2012 r. specjaliści zwrócili uwagę na mobilne wersje oprogramowania RedOctober, znanego już wcześniej z atakowania desktopów, głównie agencji rządowych i służb dyplomatycznych. W tym samym roku pojawiły się też mobilne wersje programu znanego od 2011 r. FinFisher/FinSpy – dla środowisk Androida, iOS, Windows Mobile, Symbiana i BlackBerry. Oprogramowanie to potrafiło uruchamiać ukryte połączenia w celu podsłuchu otoczenia zainfekowanego telefonu, pobierać z niego logi rozmów wychodzących i przychodzących, wiadomości tekstowe i MMS-y, śledzić współrzędne GPS właściciela telefonu i wszystkie te informacje przesyłać do centrum podsłuchu. Wersje dla poszczególnych systemów miały też dodatkowe funkcje (np. FinSpy dla Symbiana potrafił wysyłać zrzuty ekranowe, dla BlackBerry – monitorować połączenia przez BlackBerry Messengera, dla Androida – włączać i wyłączać tryb samolotowy). Programy o takich właściwościach były znane wcześniej, nowością było to, że FinSpy został opracowany przez zarejestrowaną w Wielkiej Brytanii firmę Gamma Group International, która wtedy chwaliła się na swoich stronach WWW tworzeniem dla agend rządowych zdalnych narzędzi do monitoringu.

Pierwsze informacje na temat zakupu od włoskiej firmy Hacking Team i stosowania oprogramowania RCS System szpiegującego telefony komórkowe w Polsce pojawiły się w serwisie niebezpiecznik.pl już w czerwcu 2014 r., od lipca 2015 r. w serwisie jest już widoczna faktura za zakup na kwotę 178 tys. EUR i inne szczegółowe dane, pozyskane przez… włamywaczy na serwery Hacking Team. Natomiast informacje o Pegasusie pojawiły się w serwisie

w sierpniu 2016 r., a staranny opis działania systemu – w grudniu 2019 r. Czym jest więc ów izraelski Pegaz i czy możemy się przed nim zabezpieczyć?

Malware jako broń cyberwojen

Pierwszym użyciem złośliwego oprogramowania w niewypowiedzianej czy niewidzialnej wojnie było wpuszczenie wirusa Stuxnet do lokalnej sieci sterującej wirówkami w irańskim zakładzie wzbogacania uranu. Według niepotwierdzonych (przez nikogo) danych wirus zniszczył 20% działających wirówek, co mocno przyhamowało irański program stworzenia broni nuklearnej.

W różnych serwisach omawiane są liczne przypadki ataków różnych grup formalnie niezwiązanych z żadnym rządem czy armią, choć kierunki czy obiekty ataku – albo struktury państwa „nielubianego" w jakimś kraju, albo aktywiści ruchów obywatelskich niecieszący się szczególnym uznaniem władz – mogą wskazywać na jakieś powiązania. Do takich incydentów zaliczane są m.in. zmasowane ataki DDoS na estońskie instytucje publiczne, w tym parlament i rząd, banki oraz media w kwietniu 2007 r., po przeniesieniu pomnika „Brązowego Żołnierza" na cmentarz wojskowy. Polityczną reakcją obronną NATO na ten incydent było utworzenie w Tallinie w 2008 r. NATO Cooperative Cyber Defence Center of Excellence (CCDCOE). W 2008 r. seria cyberataków poprzedziła rosyjsko-gruziński konflikt o Osetię. Co najmniej od dziewięciu lat trwają cyberataki na Ukrainę – w tym w 2015 r. ataki trojanem Black-Energy na ukraiński system dyspozycji mocy, ataki (głównie na instytucje publiczne Ukrainy) szyfrującymi lub nadpisującymi sektor MBR dysków wirusami z rodziny Pietia w 2017 r. i najnowsze (od stycznia 2022 r.) ataki na centralne rządowe strony WWW Ukrainy.

Bogatą historię ma cyberwojna między Iranem a Izraelem – choć oficjalnie rządy obu krajów zaprzeczają wszelkim medialnym informacjom na ten temat. Kilka epizodów z ostatnich lat: w kwietniu 2020 r. miał miejsce atak na sterowanie infrastrukturą wodno-kanalizacyjną w różnych miejscowościach Izraela, w odwecie w maju 2020 r. zaatakowane zostały systemy logistyczne w wielkim irańskim porcie Shahid Rajaee w Bandar Abbas nad Cieśniną Ormuz. W październiku 2021 r. zaatakowano systemy 4,3 tys. irańskich stacji benzynowych, które musiały przejść na tryb ręcznego sterowania, a przywracanie sprawności trwało 12 dni.

Jak to działa?

W 2016 r. – dawno, warto to odnotować, bo oprogramowanie szpiegujące jest cały czas aktualizowane i zmieniane – pojawiła się w Sieci w formie pliku PDF instrukcja do systemu Pegasus. Większość wiedzy o nim pochodzi właśnie stamtąd lub jest pochodną opublikowanych tam informacji, co do których nie może być pewności, czy nie są dezinformacją. Według nich Pegasus to system łączący hakerskie oprogramowanie szpiegujące oraz sprzęt do rejestracji podsłuchiwanych danych i prowadzenia korespondencji z botami zbierającymi dane, które są zwykle poprzez exploity instalowane na telefonach inwigilowanych osób. Wyczerpujące informacje na temat Pegasusa dostępne są na stronie: https://niebezpiecznik.pl/post/jak-wyglada-rzadowy-trojan-pegasus-od-srodka/).

Najczulszym punktem w działaniach tego systemu jest konieczność niezauważalnego dla właściciela zdobycia kontroli nad jego telefonem. Można to osiągnąć kilkoma metodami.

Rezydent Pegasusa wkrada się do pamięci urządzenia, najczęściej wykorzystując luki *zero-day* w systemach operacyjnych lub aplikacjach. Exploit *zero-day* działa na lukach, które do momentu jego wykorzystania nie zostały jeszcze odkryte ani przez użytkowników, ani producentów oprogramowania. Wszystko dzieje się w sposób przezroczysty i nie wymaga żadnej interakcji właściciela infekowanego smartfona. Nie zawsze jest to jednak możliwe. Wtedy sięga się po metodę fałszywej flagi, czyli np. podsuwa właścicielowi telefonu jakiś adres strony internetowej, po otwarciu której nastąpi zainfekowanie telefonu oprogramowaniem Pegasusa. Można też wykorzystać podatność komunikatorów typu iMessage, What's App czy Messenger, kiedy infekcja następuje po odczytaniu przez użytkownika fałszywej, złośliwej wiadomości (również SMS). Te sposoby mają jednak tę wadę, że wymagają interakcji właściciela urządzenia. Musimy podsunąć mu link czy wysłać wiadomość skłaniającą do kliknięcia. Nie jest to banalne zadanie, trzeba więc szczegółowo je opracować, najlepiej wykorzystując informacje zdobyte wcześniej innymi metodami obserwacji. Poza tym takie sposoby pozostawiają już pewne ślady w telefonie.

Istnieje jeszcze inna metoda zainstalowania Pegasusa – wykorzystanie ataku przeprowadzonego tzw. sposobem Man-In-The-Middle poprzez fałszywy BTS, czyli urządzenie zwane IMSI Catcherem. Takie urządzenie włącza się pomiędzy nasz telefon a stację bazową (BTS) operatora, przechwytując całą komunikację naszego smartfona z prawdziwym BTS-em. W ten sposób można nie tylko podsłuchiwać i nagrywać rozmowy, lecz także podsunąć fałszywe połączenie do złośliwej strony infekującej Pegasusem. Tu oczywiście potrzebna jest cała operacja, gdyż fałszywy BTS musi znaleźć się w odpowiednim miejscu, żeby został wykryty przez telefon ofiary i umożliwił wykonanie zadania. Innymi słowy, trzeba jeździć za telefonem, który chcemy podsłuchiwać.

Jest to nieco prostsze od zorganizowania odpowiedniej prowokacji i zainstalowania agenta Pegasusa ręcznie na wybranej komórce. Manualna instalacja trwa około 5 minut i operator musi mieć dostęp do urządzenia ofiary przez cały ten czas. W grę wchodzą scenariusze rodem z książek szpiegowskich:

- zaproszenie kogoś do miejsca, gdzie telefony zostawia się w „depozycie";
- podstawienie agenta (osoby), która uwiedzie/upije/uśpi ofiarę lub będzie w pomieszczeniu z ofiarą, kiedy ta bierze prysznic;
- kontrola drogowa „ze sprawdzeniem; czy telefon nie jest kradziony". Nigdy nie oddawajcie swoich telefonów nawet najbardziej nieporadnie wyglądającemu policjantowi – na tylnym siedzeniu jego policyjnego radiowozu może siedzieć niewidoczny operator Pegasusa – ostrzega niebezpiecznik.pl.

Jak widzimy, wachlarz sposobów zainfekowania smartfona jest wystarczająco szeroki, żeby potencjalną ofiarę można było próbować osaczyć z wielu stron, więc uniknięcie szpiegowania jest bardzo trudne. Biorąc pod uwagę, że Pegasus stosowany jest głównie przez służby państwowe, które mają olbrzymie możliwości i doświadczenie operacyjne, a także zasoby finansowe pozwalające na stosowanie najbardziej wyrafinowanych i kosztownych rozwiązań, to szanse na uniknięcie inwigilacji są naprawdę nikłe. Z drugiej strony opracowanie i zastosowanie exploita typu *zero-day* nie jest takie łatwe, wymaga naprawdę wielu, często bardzo kosztownych zabiegów, a inne sposoby, mogą wymagać interakcji z użytkownikiem i zostawiają więcej śladów w smartfonie. Dlatego nie należy się z góry załamywać omnipotencją służb, tylko stosować pewne zasady „cyfrowej higieny" swojego telefonu, które mogą w pewnych przypadkach znacząco zmniejszyć niebezpieczeństwo niezauważalnego zainstalowania na nim śledzącego nasze dane oprogramowania.

Jak się bronić?

Podstawowe „zasady higieny" smartfona, niezależne od producenta telefonu i systemu operacyjnego, zestawiliśmy w krótkiej ramce. Każdy z wymienionych punktów wymaga pewnych poświęceń z naszej strony, jednak specjaliści upierają się, że jeśli poważnie traktujemy zagrożenie inwigilacją, powinniśmy równie poważnie potraktować konieczność zastosowania każdego z nich w codziennej praktyce. Oczywiście stosowanie nawet całej siódemki najprawdopodobniej nie uchroni nas przed inwigilacją, jeżeli „ktoś" bardzo potrzebuje nas wyśledzić, jednak utrudni „ktosiowi" życie, a także przyczyni się do łatwiejszego zlokalizowania i wykrycia ewentualnej infekcji.

Na smartfonach Apple dodatkowo zaleca się wyłączenie usługi iMessage, która jest bardzo podatna na ataki z zewnątrz. To również trudna decyzja, gdyż jest to usługa wygodna. W „zasadach higieny" chodzi jednak o to, żeby wyeliminować słabe punkty, przez które najczęściej dochodzi do spenetrowania zawartości smartfona. Niestety, takie wygodne, dobre usługi, zwłaszcza domyślnie włączone i właściwie niekontrolowane przez użytkownika, często stają się nośnikiem infekcji różnego typu. Podobnie jednymi z najbardziej niebezpiecznych pod tym względem są domyślne przeglądarki internetowe, dlatego zaleca się stosowanie alternatywnych wobec nich rozwiązań. Mimo że te alternatywne przeglądarki korzystają zwykle z tego samego silnika, co przeglądarka domyślna, okazują się nieraz bardziej odporne na działania hakerskie.

Szczęśliwa siódemka przeciw Pegazom z CBA

1. **Codziennie restartuj telefon.**
2. **Włącz blokadę ekranu.**
3. **Nie zapominaj o aktualizacji nie tylko systemu operacyjnego, lecz także innego oprogramowania.**
4. **Staraj się nie klikać w linki otrzymane SMS-em, bądź np. e-mailem bez uprzedniej weryfikacji.**
5. **Używaj alternatywnych przeglądarek internetowych.**
6. **Zainstaluj na smartfonie pakiet oprogramowania antymalware i antywirusowego.**
7. **Używaj zaufanych usług VPN.**

Starajmy się też nauczyć nie wchodzić bezmyślnie na strony internetowe, do których linki dostajemy SMS-em. Choćby wiadomość wyglądała bardzo wiarygodnie i idealnie trafiała w nasze oczekiwania, czy też np. lęki, to lepiej powstrzymać pokusę wejścia pod podany adres i postarać się go wcześniej zweryfikować, np. na komputerze stacjonarnym, jeśli uważamy, że otrzymany link może dotyczyć czegoś naprawdę istotnego. Podobnie uważajmy na e-maile i innego typu wiadomości z linkami. Generalnie unikajmy wchodzenia pod nieznane adresy internetowe. A przynajmniej czytajmy adresy przed kliknięciem w link, bo czasem ich składnia od razu sugeruje jakieś oszustwo i wystarczy odrobina spostrzegawczości, żeby uniknąć kłopotów.

Stosujmy pakiety antywirusowe i antymalware. Mają one swoje wady, zwłaszcza ich metody heurystyczne generu-

Skrzydlaty koń czy konsola do gier

Mityczny heros Bellerofont na skrzydlatym Pegazie chciał wjechać na Olimp, jednak Pegaz dotarł na szczyt bez jeźdźca. W nagrodę Zeus przeniósł Pegaza na nieboskłon, gdzie rezyduje do dziś. Tamten Pegaz jest dość dobrze znany, przynajmniej tym, którzy odebrali staranniejsze wykształcenie, ewentualnie pamiętają go z czołówki dawnego programu kulturalnego TVP. Natomiast nie wszyscy, którzy niedawno szukali w piwnicach konsoli do gier Pegasus, wiedzą, że nazwę tę nadano jednemu z tajwańskich klonów sławnego Famicona japońskiej firmy Nintendo. Oryginalnego Famicona w latach 1983–1995 sprzedano na świecie prawie 62 mln sztuk, a jego klonów produkowanych nie tylko na Tajwanie, lecz nawet w Brazylii i w Rosji, nikt nie zliczy. Klon Famicona pod nazwą Pegasus był niezwykle popularny w pierwszej połowie lat 90. XX w. nie tylko w Polsce (dzięki importerowi, firmie BobMark International), lecz także w ówczesnej Czechosłowacji i Jugosławii.

W latach świetności Famicona i Pegasusa nikt nie miał zamiaru używać ich jako broni, skupiano się raczej na zdobywaniu cracków do gier. Najsłynniejszą grą na platformę Famicona i jego klony, w tym Pegasusa, była „Super Mario Bros" – gra o braciach Mario i Luigim, uważana za „grę wszechczasów". Przepisywano ją i importowano na wszelkie możliwe platformy sprzętowe i systemowe; na same tylko dystrybucje Linuksa powstało kilkadziesiąt wersji, co rozszerza możliwości grania w nią nawet na superkomputerach. Oczywiście są też wersje Super Mario Bros na dwa główne środowiska smartfonowe – Androida i iOS.

ją sporo fałszywych alertów, ale stanowią jednak dodatkowy element zabezpieczający. Np. producent pakietu Bitdefender chwali się na swoich stronach internetowych, że od 2017 r. jego oprogramowanie przechwytuje exploity Pegasusa. Ile jest w tym prawdy – trudno zweryfikować. Choć pełna skuteczność wydaje się nieprawdopodobna, to mogły zdarzyć się przypadki wykrycia przez Bitdefender obecności Pegasusa na telefonach. Programy tego typu mogą również znaleźć pewne przesłanki wskazujące na penetrację naszego telefonu, np. wykryć zdalny jailbreak na iPhone'ach. Warto też wspomnieć, że istnieje opracowane pod auspicjami Amnesty International (dostępne za darmo na GitHubie https://github.com/mvt-project/mvt) narzędzie MVT (Mobile Verification Toolkit), które dokonując analizy różnych śladów w telefonie, ocenia, czy był on szpiegowany czy nie. Jest to jednak raczej narzędzie profesjonalne, którego zastosowanie wymaga doświadczenia i wiedzy kryminalistycznej.

Stosowanie wirtualnej sieci prywatnej, czyli tunelowania naszej komunikacji najlepiej połączonego z szyfrowaniem transmisji, przydaje się zwłaszcza w przypadku, kiedy korzystamy z hotelowych czy dworcowych sieci Wi-Fi. Ogólnie nie zaleca się korzystania z takich sieci, jednak przy zastosowaniu VPN zagrożenie jest znacznie mniejsze. VPN pomoże także np. w przypadku zastosowania wspomnianego w artykule IMSI Catchera, czyli fałszywego BTS. Warto tu zauważyć, że najlepsze usługi VPN są płatne, więc jeśli chcemy się dobrze zabezpieczyć, musimy liczyć się z wydaniem pewnej sumy na abonament.

Jak i przed czym bronią się rządy?

W lipcu 2021 r. brytyjski dziennik „Guardian" opublikował kilka oficjalnych odpowiedzi na pytania dziennika zadane rządom krajów, których obywatele znaleźli się na listach ofiar stosowania Pegasusa, opublikowanych przez serwisy Amnesty International, oraz inicjatywy Pegasus Project wspólnego przedsięwzięcia 17 redakcji (w tym „Guardiana") i organizacji Forbidden Stories, zajmującej się badaniem działań przeciwko dziennikarzom. Lektura tych wyjaśnień jest pouczająca:

- „Indie to silna demokracja, która jest zaangażowana w zapewnienie wszystkim swoim obywatelom prawa do prywatności jako prawa podstawowego. Realizując te zasady, Indie uchwaliły ustawę o ochronie danych osobowych z 2019 r. oraz zasady dotyczące technologii informacyjnej (wytyczne dla pośredników i kodeks etyki mediów cyfrowych) z 2021 r. w celu ochrony danych osobowych osób fizycznych i wzmocnienia pozycji użytkowników platform mediów społecznościowych. (…) Zobowiązanie do wolności słowa jako podstawowego prawa jest kamieniem węgielnym indyjskiego systemu demokratycznego (…). Jednak z ankiety wysłanej do rządu Indii wynika, że konstruowana historia jest nie tylko pozbawiona faktów, ale także oparta na z góry przyjętych wnioskach. Wygląda na to, że autorzy pytań próbują się wcielić jednocześnie w rolę śledczego, prokuratora, a także ławę przysięgłych (…). Reakcja rządu Indii na informacje na temat korzystania z Pegaza była szeroko komentowana przez media i sama w sobie jest wystarczająca, aby przeciwdziałać wszelkim złośliwym twierdzeniom o rzekomym związku między rządem Indii a Pegazem. (…) Zarzuty dotyczące rządowej inwigilacji konkretnych osób nie mają żadnych konkretnych podstaw".

- Maroko: „Władze Maroka nie rozumieją kontekstu prośby międzynarodowego konsorcjum dziennikarzy Forbidden Stories, domagającego się odpowiedzi i wyjaśnień od rządu marokańskiego dotyczących narzędzi cyfrowego nadzoru NSO Group. Przypominamy, że bezpodstawne zarzuty opublikowane przez Amnesty International i przekazane przez Forbidden Stories były już przedmiotem oficjalnej odpowiedzi władz marokańskich, które kategorycznie zaprzeczyły takim zarzutom".

- Węgry: „Nic nie wiemy o jakimkolwiek rzekomym gromadzeniu danych, o które wystąpiono we wniosku. Węgry są demokratycznym państwem prawa i jako takie zawsze działały i nadal działają zgodnie z obowiązującym prawem. Na Węgrzech organy państwowe uprawnione do stosowania tajnych instrumentów są regularnie monitorowane przez instytucje rządowe i pozarządowe. Czy te same pytania zadane zostały rządom Stanów Zjednoczonych Ameryki, Wielkiej Brytanii, Niemiec czy Francji? Jeśli tak, jak długo zajęła im odpowiedź i jak zareagowały? Czy w formułowaniu pytań wspomagała konsorcjum jakaś służba wywiadowcza?"

Kilka krajów, do których się zwrócono (Azerbejdżan, Bahrajn, Dubaj, Kazachstan, Meksyk i Zjednoczone Emiraty Arabskie), nie odpowiedziało na pytania.

Konsorcjum otrzymało też kilka pism od NSO Group ze stwierdzeniami, że raport konsorcjum oparty jest na „błędnych założeniach" i „niepotwierdzonych teoriach", a analiza danych przez dziennikarzy uczestniczących w Projekcie Pegasus opierała się na „błędnej interpretacji danych, które wyciekły z dostępnych i jawnie podstawowych informacji, takich jak usługi HLR Lookup, które nie mają wpływu na listę celów Pegasusa lub nabywców jakichkolwiek innych produktów NSO".

W Polsce w styczniu br. Jarosław Kaczyński potwierdził, że polskie służby zakupiły i używają Pegasusa. Pytany o wizytę deputowanych Parlamentu Europejskiego – pod przewodnictwem hiszpańskiego europosła Estebana Gonzaleza Ponsa – która ma na celu „zbadanie nielegalnej inwigilacji opozycji przy użyciu Pegasusa" powiedział (16 lutego br.): – *To trzeba traktować jako wyjście przed szereg jakiegoś bardzo słabego, jeśli chodzi o umiejętności polityczne, i mało znanego hiszpańskiego europarlamentarzysty. Nie przypisywałbym temu faktowi większego znaczenia. Natomiast tendencja istnieje i trzeba się przed tym bronić*.

Cyberarmie

- **Od dłuższego czasu w armiach różnych krajów powstają oficjalnie lub nieoficjalnie „cyberkompanie", „cyberpułki" albo nawet „cyberdywizje". Długa lista cyberjednostek i agencji 77 krajów – od Albanii po Wietnam – jest w Wikipedii pod adresem https://en.wikipedia.org/wiki/List_of_cyber_warfare_forces. Z polskich instytucji wymieniono na niej: Centrum Operacji Cybernetycznych, Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni oraz Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe SKW/MON, obecnie wszystkie pod adresem https://www.cyber.mil.pl.**

- **Militarnymi siłami informatycznymi dysponują oczywiście znane potęgi militarne i informatyczne – USA, Rosja, Chiny czy Izrael, w którym w 2020 r. w firmy sektora cyberbezpieczeństwa zainwestowano 2,9 mld USD, co stanowiło 31% inwestycji w całym tamtejszym sektorze IT. Jednostka teleinformatyczna C4I armii izraelskiej chlubi się tradycjami jednego ze swych poprzedników – utworzonej w 1937 r. służby telekomunikacyjnej Hagany, paramilitarnej organizacji z czasów brytyjskiego Mandatu Palestyny. Jednostka telekomunikacyjna już w tym samym roku zorganizowała kurs dla radiotelegrafistów, dysponowała 12 tajnymi radiostacjami, a dla uniknięcia brytyjskich podsłuchów w 1938 r. wdrożyła do służby 150 gołębi pocztowych. Po proklamowaniu w 1948 r. państwa Izrael stanowiła podstawę jednostek teleinformatycznych Sił Obronnych Izraela.**

- **Według raportu Amnesty International w 2017 r. zastępca szefa zarządu politycznego armii wietnamskiej ogłosił powstanie specjalnej jednostki informatycznej, zwanej przez aktywistów ruchów obywatelskich „Force 47", w skład której weszło ok. 10 tys. specjalistów.**

- **Neutralna od pierwszej połowy XIX w. Szwecja (ostatnią wojnę prowadziła przez trzy tygodnie w 1814 r. z... Norwegią) w 1954 r. podpisała tajne porozumienie z USA, Wielką Brytanią, Kanadą, Australią i Nową Zelandią zwane Sojuszem Pięciorga Oczu, na podstawie którego szwedzka Agencja Wojskowego Rozpoznania Radioelektronicznego (FRA) Ministerstwa Obrony, podsłuchująca kogo się tylko da, przekazuje wyniki podsłuchu wywiadom krajów porozumienia. Według szwedzkiej ustawy o totalnej obronie z grudnia 2021 r. budżety szwedzkich cyberjednostek, tworzonych w ramach projektów ITF i 2ITF i współpracujących z FRA oraz z agencjami wywiadu, mocno zwiększono już od 2021 r.; mają one osiągnąć pełną zdolność obronną (bojową?) – a więc przede wszystkim odpowiednie stany osobowe – do 2027 r.**

- **NATO poświęca coraz więcej uwagi nowym obszarom cyberobrony związanym np. z komputerami kwantowymi i biotechnologiami kognitywnymi (CBT).**

Instalowanie nowej rzeczywistości

Człowiek (…) wytwarza sobie pewną zupełnie nową rzeczywistość lub quasi--rzeczywistość. Raz wytworzona, stanowi ona potem znamienny składnik otaczającego go świata[1].

Ada Florentyna Pawlak

antropolożka technologii, prawniczka i historyczka sztuki. Wykładowczyni akademicka (IEiAK UŁ, Artes Liberales UW, Wydział Zarządzania UŁ, Akademia im. Leona Koźmińskiego w Warszawie, „Trendwatching & Future Studies" na Wydziale Humanistycznym AGH w Krakowie), popularyzatorka nauki i spikerka w obszarze społecznych kontekstów nowych technologii i towarzyszących im idei. Specjalizuje się w dyskursach kapitalizmu afektywnego, kultury cyfrowej, transhumanizmu i sztucznej inteligencji, technointymności, współpracy człowieka z maszyną i projektów art@science. Współpracuje z Digital University, Polsko-Amerykańską Fundacją Wolności, Rzecznikami Nauki i łódzkim Fotofestiwalem.

1 R. Ingarden., *Książeczka o człowieku*, PWN, Warszawa 1973, s. 29-30.

Istnieją światy, które spełniają się w wyobraźni. Nie można w nie wkroczyć, zanurzyć się, zamieszkać. Mimo to fascynacja mitycznymi, niezwykłymi krainami, egzotyczne opowieści o niezwykłych lądach, hiperbolizowane relacje z dalekich wypraw – to rzecz równie stara, jak ludzka potrzeba oderwania się od „tu i teraz", niezależna od szerokości i długości geograficznej. Informatyczno-komunikacyjne techniki cyfrowe, globalizacja i hybrydyzacja mediów umożliwiły powstanie nowej formacji kulturowej – cyberkultury, która wyznacza planetarną perspektywę.

> *Dziś to nie maszyny pozwalające docierać do nieznanych światów stały się ośrodkiem zainteresowania wielkiego kapitału, lecz sztuczne światy, trójwymiarowe cyfrowe lądy i obiekty generowane w wirtualnych przestrzeniach, które użytkownicy mogą eksplorować za pomocą stworzonego przez siebie awatara.*

Metarzeczywistość to trwały, symulowany świat, którego doświadczają jednocześnie duże grupy użytkowników połączonych silnym poczuciem wzajemnej obecności. Może być w pełni wirtualny i samowystarczalny lub istnieć w postaci warstw wirtualnej zawartości rozszerzających rzeczywisty świat. Ostatecznym celem nie jest rzeczywistość wirtualna lub rozszerzona, lecz rzeczywistość mieszana (MR – *mixed reality*) – połączenie świata cyfrowego i rzeczywistego, które staną się nie do odróżnienia. Internet wyleje się z naszych telefonów i komputerów i połączy się z fizyczną rzeczywistością – otoczy nas, a nasze życie, praca i wypoczynek będą odbywać się wewnątrz sztucznego świata, radykalne przekształcając społeczeństwa. Zanurzenie w metaświaty cechować się będzie spójnością doświadczenia, intersubiektywnością i rygorystycznym obowiązywaniem reguł charakterystycznych dla danej symulacji, tworząc rzeczywisty obszar działań. Dzięki możliwości interakcji i braku nieograniczonej dowolności wytworzyć może się bardzo silna, intersubiektywna, konsensualna halucynacja: metarealizm. Czy dzięki technologii metaświaty będą z łatwością przechodzić kartezjański „test realnego", w którym stałość, spójność i trwałość to oznaki świata realnego, zaś przemijalność – cechą rzeczy będących jedynie zjawiskami?

Bramy do metawersum

Organizującą rolę w badaniach nad rzeczywistością wirtualną odgrywa zestaw takich pojęć, jak: immersja, interaktywność, sztuczność, teleobecność czy symulacja. To dzięki wdrożeniu umożliwiających je technologii nowa antroposfera ma być atrakcyjniejsza niż Web 2.0. Media immersyjne odnoszą się do treści cyfrowych prezentowanych użytkownikom z perspektywy pierwszej osoby, dając złudzenie, że użytkownicy są obecni w treści, a nie obserwują ją z zewnątrz. Interaktywność to stopień, w jakim użytkownik może uczestniczyć w zawartości zmediatyzowanego środowiska w czasie rzeczywistym. Jej zakres określony jest przez liczbę atrybutów, którymi można manipulować w metaświecie. Symulacja to odtwarzanie właściwości obiektów rzeczywistych w środowisku cyfrowym, tworzenie jakościowych przedstawień będących kopią zjawisk realnych bądź tworem oryginalnie niewystępującym w świecie fizycznym.

Fundamentem pod budowę nowej antroposfery są: kryptoekonomia, pojawienie się DAO (*Decentralized Autonomous Organization* – wywodzących się z koncepcji Web3 organizacji zarządzanych przez społeczność) i potrzeba kreacji nowej hierarchii – statusów społecznych, które można zmonetyzować. Cyfrowy system kastowy potrzebuje nowych narzędzi służących „chwalbie soboście", a kapitalistyczna nadkonsumpcja domaga się niematerialnych towarów. Dlatego metaświaty wznoszą się na założeniach nowej ekonomii NFT – ekosystemie uwierzytelniania np. dzieł sztuki, kolekcji, a także tożsamości. Dzięki tokenom metaposiadacze będą mogli zaprezentować swoje portfele, informując o ich geolokalizacji, historii i kontekście kulturowym powstania przechowywanych w nich obiektów.

> *Kiedy sztuczność przestaje być zauważalna i odczuwalna a środowisko nabiera cech realności, możemy mówić o doskonałej symulacji: hiperrzeczywistości – przestrzeni, w której technologie komunikacyjne dostarczają intensywniejszych i bardziej pociągających doświadczeń niż realna codzienność.*

Wynalazki techniczne to tylko jedna z dróg wiodących do metawersum. Innowacja zakłada konieczność połączonego systemu wartości, przekonań, kulturowych symboli danej społeczności, jak również ekonomii umożliwiającej funkcjonowanie w metaświecie. Zbliżają nas doń wielowymiarowe zmiany w obrębie rzeczywistości, tj. kultura komunikacji obrazowej, epidemia covid oraz epidemia samotności i narcyzmu, mające źródło w architekturze mediów społecznościowych.

Apokalipsa w pięciu smakach

Każda epoka wytwarza specyficzne tematy i narzędzia, wokół których koncentruje się ucieczka od rzeczywistości. Konsumpcja rozrywki to *modus operandi* współczesnej kultury ukierunkowanej na natychmiastowe zaspokojenie ludzkich namiętności. Fenomenu popularności makiet rzeczywistości nie sposób rozpatrywać w oderwaniu od mentalnego oprogramowania najmłodszego pokolenia i objęcia ich afektywnej perspektywy. Tworzeniu kolektywnej iluzji światów zastępczych sprzyja *modus vivendi* pokolenia cyfrowych tubylców (*digital natives*): „kultura obrazu edytowalnego" rodzi postawy eskapistyczne. Perspektywę życia we wtórnych

światach przybliża też klimatyczno-pandemiczno-polityczny pesymizm, zwiastujący „apokalipsę w pięciu smakach". Dlatego metaświaty, obiecujące ekscytujące doświadczenia, stają się uprzywilejowane poznawczo i emocjonalnie.

> *W sztucznym świecie możemy zostać kim chcemy, zmienić się w kogo zapragniemy – to sklep potrzeb tożsamościowych atrakcyjny dla uczestnika kultury, której życie społeczne i gospodarcze obraca się wokół wizerunku i bycia oglądanym. Światy zastępcze oferują iluzje omnipotencji i kontroli, nieruchomego czasu, wiecznego piękna i życzeniowego przeobrażania rzeczywistości.*

Gra i zabawa jako źródło metaświata

Web 2.0 zbudowali twórcy stron internetowych, metawersum jest natomiast tworzone przez twórców gier. „Transhumanist Art Statement" już w latach 90. domagał się przejęcia sztuki przez nowych projektujących światy artystów, wskazując, że transludzka estetyka i ekspresja powinny połączyć się z nauką i technologią w celu zwiększania doznań zmysłowych. Zadaniem twórców nie będzie tworzenie tradycyjnych dwuwymiarowych dzieł, lecz kreacja narzędzi, za pomocą których użytkownicy wchodzą w interakcję z treścią. Metarodowici uznają to za całkowicie naturalne, ponieważ droga do światów zastępczych poprowadzi ich przez grę i zabawę. Fortnite, Minecraft czy Roblox pod maską gry są przestrzennymi środowiskami, w których młodzi ludzie spotykają się i uczestniczą w wydarzeniach. Decentraland, The Sandbox, światy powstające w Epic Games, Niantic, Nvidia czy Microsoft, wpływają na sposób, w jaki młodzież nawiązuje kontakty towarzyskie, gromadzi się w społecznościach, tworzy relacje ekonomiczne i styl myślenia o pracy i zarabianiu pieniędzy dzięki nowym zawodom.

Kategorie zabawy i gry wiąże się z powoływaniem „osobnego świata", rządzącego się odmiennymi prawami i pozostającego poza zwykłym życiem. Holenderski historyk Johan Huizinga już ponad 80 lat temu zaproponował całościową interpretację kultury, w której kategoria zabawy zajmuje centralne miejsce, a skłonność do zabawy stoi u źródeł wszelkich ludzkich zachowań społecznych. Sytuuje się ona poza sferą aktywności wynikających z dążenia do przetrwania, co nie zmienia faktu, że może być sprawą śmiertelnie poważną, jak wszelka niepoddana ograniczeniom władza.

Cyborgiczny tour de monde

Nasze poczucie rzeczywistości tworzy się dzięki ucieleśnionym interakcjom, w które wchodzimy z otoczeniem. Migracji umysłów do metawersum towarzyszyć musi proces cyborgizacji, który w pierwotnych koncepcjach wiązał się z przebudową organizmu ludzkiego w celu przystosowania go do trudnego dla ludzkiej biologii otoczenia poprzez wymianę niektórych organów na sztuczne lub dodanie elementów wzmacniających ludzkie możliwości.

Człowiek w metaświecie będzie zestawionym z biologicznego organizmu i zewnętrznych zasobów sprzężonym systemem, tworzącym nowy układ poznawczy. Aby całkowicie się zanurzyć w symulacji, potrzebujemy sprzętu w postaci urządzeń ubieralnych: gogli VR, soczewek/okularów z AR czy rękawic, dzięki którym poczujemy wirtualne przedmioty. Ciało będzie przemierzać sztuczną przestrzeń, odbierając i reagując na bodźce dzięki dedykowanym urządzeniom – hełmom, bieżniom, rękawicom, skafandrom. Celem tej technologii jest osiągnięcie pełnego zanurzenia zmysłowego, przekierowanie sensorium tak, by odbierało bodźce z generowanego przez komputer środowiska cyfrowego. Postludzkie ucieleśnienie oferuje możliwość pojawienia się wtórnej oralności dzięki bezpośredniej komunikacji przywracającej dźwięk i gesty ludzkiego sensorium w miejsce zapośredniczonej znakiem komunikacji symbolicznej.

Metahumans – postludzkie wizerunki bez podmiotu

Neal Stephenson ukuł termin „metaverse", opisując wirtualny świat 3D, w którym awatary mogą wchodzić w interakcje ze sobą i sztucznie inteligentnymi agentami. Cyfrowy wieloświat zamieszkany będzie nie tylko przez naszych cyfrowych bliźniaków, lecz również przez atrapy stworzenia. Wiele firm podjęło już inwestycje w kreację przyszłych mieszkańców nowej antroposfery – cyfrowych postludzi (DPH – *Digital Posthumans*).

Silnik personalizacji awatarów to patent Mety – globalnego programu klonowania ludzi. Ma pozwolić na tworzenie trójwymiarowych postaci na podstawie zdjęć użytkowników i tzw. replikatora skóry. Cenny patent z zakresu fotogrametrii, pozwalającej tworzyć hiperrealistyczne awatary użytkowników, ma polska firma Wolf 3D: https://wolfstudio.pl/2-digitalizacja-3d. Natomiast Inworld AI to platforma do budowania sztucznych ludzi i „mózgów" wirtualnych postaci mających wypełnić wirtualne środowiska: https://www.inworld.ai. Wiodące firmy na globalnym rynku cyfrowych ludzkich ucieleśnień to: UneeQ, Microsoft, Didimo, HOUR ONE AI, Spatial Systems, CARV3D, DeepBrain AI, Soul Machines, Synthesia.

Wśród *metahumans* znajdą się hiperrealistyczne awatary (patrz ramka powyżej), będące alter ego użytkownika, jak

również wygenerowani komputerowo sztuczni ludzie (VB – *Virtual Being*) – wizerunki bez podmiotu mającego odpowiednik w świecie fizycznym. Te istoty wirtualne będą mieć formę cielesnej naoczności, choć brak im materialnego, somatycznego odpowiednika – ich istnienie wyczerpuje się na byciu spostrzeganym. Hiperrealistyczny symulakr będzie wchodził w interakcje, inicjował procesy – jego istotą jest bycie w relacji. Istoty wirtualne działać będą w mediach komunikacyjnych (gwiazdy, idole), świadczyć usługi profesjonalne (lekarze, nauczyciele) i dotrzymywać towarzystwa. Sztuczni ludzie, domagający się podmiotowego traktowania, przebudują nasze społeczne relacje.

Symulacja więzi i zarażanie afektywne

W praktykach społecznych istotne jest współdzielenie zamieszkiwanej rzeczywistości. Wspólnoty w metaświatach, niezależnie od dzielącej je przestrzeni, konstruowane będą wokół rozmaitych przepływów: informacji, kapitału interakcji, kultury. Kreacja metahumans to odpowiedź na ludzką potrzebę afiliacji, bezpieczeństwa, pragnienie akceptacji, troski, szacunku i społeczne zobojętnienie w kulturze narcyzmu. Ich *telos* to ochrona człowieka przed uczuciem pustki. W świecie antropomorficznych atrap będziemy nieustannie narażeni na eksploatację emocjonalną ze strony programów, których architektura wykorzystuje znajomość naszej biologii.

Pojawiwszy się w metaświecie nie będziesz czuł się samotny, nieszczęśliwy – zostaniesz przywitany, otoczony uwagą przez istoty wirtualne symulujące ludzi. Ten syntetyczny stan czuwania ku innemu może okazać się niezwykle atrakcyjny w zestawieniu z obojętnością ludzi. To z tego powodu nastąpić może „osobliwa podmiana" – w miejsce żywej osoby i fizycznego ciała pojawi się idealny obraz – użytkownik może preferować ideał w miejsce rzeczywistości. Metaświat będzie nie tylko konstelacją obiektów , lecz także quazi-podmiotów, z którymi będziemy czuć się związani. Nadanie znamion realności pozorom rodzi ryzyko podszywania się atrap pod formy ożywione.

Cyberimmortalizm

Pojęcie allotopii (αλλότοπία), denotujące „miejsce inne", topograficzne „tam, gdzie jest inaczej niż tu" jest jednym ze sposobów dokonywania transfiguracji rzeczywistości, obok uchronii, metatopii, metachronii czy utopii[2]. Allotopia tworzy świat alternatywny i sprawia, że jest on bardziej realny niż świat rzeczywisty. Po zanurzeniu się weń przestaje nas interesować jego relacja ze światem rzeczywistym. Aby w światach nierzeczywistych dopatrywać się wyższego progu realizmu niż w świecie faktycznym, człowiek musi zrealizować w nim potrzeby zdiagnozowane przez Maslowa: bezpieczeństwa, przynależności, uznania, samorealizacji. Metawersum to wielki mit stworzenia wieku informacji – projekt metafizyczny mówiący o kreacji światów, naturze rzeczywistości, fundamentach bytów i relacji między ciałem i umysłem. Systemy komputerowe tworzące środowiska cyfrowe pełnią dziś funkcję ontyczną, generując obszary i przedmioty będące funkcjonalnymi cyfrowymi odpowiednikami bytów fizycznych, podtrzymując w istnieniu nowe metarzeczywistości.

Refleksja nad śmiertelnością, istotna dla poszukiwania sensu i sposobów bycia w świecie, od najdawniejszych czasów przybiera rozmaite kształty pod wpływem zmiennych prądów filozoficznych i cywilizacyjnych trendów. Zauważmy, że w kulturze podporządkowanej pierwiastkowi technicznemu członkowie społeczeństwa muszą wierzyć, że spełnienie jest osiągalne tu i teraz, że nie jest konieczny system rytuałów dedykowanych pozaświatowym siłom. Metafizyczne laboratorium złoży ofertę pośmiertnego uobecnienia w symulacji w formie awatara, przekształcając z czasem nasz stosunek do śmierci i żałoby. Sztuczne twory, udając życie, zaburzą tradycyjny podział na byty żywe i martwe.

Deep Fake Culture w maszynie doświadczeń

W sztucznych światach upadną znane porządki reprezentacji i wypłaszczą się ontologie. Użytkownicy będą potrójnie łudzeni: co do ich fizycznego otoczenia, co do ich własnych ciał i wrażeń zmysłowych oraz tożsamości innych podmiotów. W metaświecie zdolności interpretowania doświadczeń należy odrzucić jako niewiarygodne, ponieważ w nowym środowisku, w którym obowiązują inne prawa, nie ma podstaw do ufania swojemu dotychczasowemu doświadczeniu. Metaświat pogłębi „kryzys epistemiczny" powstały w kulturze postprawdy.

Filozof Robert Nozick zapytał, czy wolelibyśmy żyć w prawdziwym świecie, czy w rzeczywistości niekończącej się przyjemności oferowanej przez „maszynę doświadczeń", zapewniającą pełną immersję tak, że niemożliwe staje się odróżnienie wygenerowanych wrażeń od prawdziwego życia. Eksperyment zaprojektowano, aby pokazać ograniczenia „hedonizmu" – idei, że ludzie są przede wszystkim motywowani do szukania przyjemności, że bardzo niewielu z nas wybrałoby życie w ciągłej przyjemności (o ile byłaby fałszywa), ponieważ ludzie wydają się być zaprogramowani na pragnienie prawdy. Już wkrótce będziemy mieli szansę sprawdzić, czy mogąc żyć w sztucznych rajach wybierzemy rzeczywistość „pierwszego rzędu", czy urządzimy się w kulturze głębokiego fejku (*Deep Fake Culture*).

---

2 W badaniach literackich zaadaptowane za sprawą referatu „Scienza e fantascienza" Umberta Eco z 1984 r., funkcjonującego w Polsce po tytułem „Światy science fiction". K.M. Maj, Allotopia – wprowadzenie do poetyki gatunku, *Zagadnienia Rodzajów Literackich* 2014, t. 57, nr 1, s. 89-105.

Mistyczny wymiar metawersum

Zgłoszony przez Facebook i Marka Zuckerberga projekt stworzenia nowej wirtualnej przestrzeni do kontaktów międzyludzkich o niespotykanej intensywności doznań i przeżyć – szumnie nazwany metawersum (drugim poziomem wirtualnej rzeczywistości) – jest kolejnym zabiegiem giganta informatycznego o pozyskanie rynku usług komputerowych.

W niektórych elementach projektu kryją się treści warte namysłu co do jego skutków dla życia społecznego, są bowiem kontrowersyjne.

Jak głęboko zanurzyć się w VR

Podstawą funkcjonowania metawersum jest *immersja*, jakiej mają doświadczyć, na niespotykaną dotychczas skalę, użytkownicy urządzeń i aplikacji, głównie gogli i symulatorów VR. Zauważmy, że immersja jako wielozmysłowe, intensywne i dojmujące przeżycie wyobrażeniowo-emocjonalne jest rodzajem doświadczenia, które nie musi być wywołane wyłącznie narzędziami informatycznymi.

Badacze kultury i cywilizacji już od dawna, zaś psychologowie od paru dekad, i to na podstawie badań empirycznych, stwierdzają, że immersyjne skutki miały już na początku

Marek Hetmański

profesor zwyczajny w Instytucie Filozofii Uniwersytetu Marii Curie-Skłodowskiej, kierownik Katedry Ontologii i Epistemologii, członek Polskiego Towarzystwa Filozoficznego i Polskiego Towarzystwa Kognitywistycznego. Filozof i epistemolog, zajmuje się problemami poznania i wiedzy w ich uwarunkowaniu społecznym oraz technicznymi czynnikami, w tym zwłaszcza technologiami informatycznymi.

cywilizacji pieśni, opowieści, przemowy, monologi, a także epicka i fabularna literatura, dramaty sceniczne, filmy, w końcu gry komputerowe. Wszystkie te przekazy, z racji tego, że silnie oddziałują na wyobraźnię słuchaczy lub widzów, dając im intensywne i wciągające odczucie obecności w rzeczywistości innej niż realna, są ze swej natury immersyjne. Wywołują wrażenie przejścia między odmiennymi środowiskami, które jest nagłe, stopniowe albo też powolne, pełne lub częściowe. Istotą immersji jest także to, że ten, kto jej doświadcza – mimowolnie, z zamiarem szczególnego przeżycia lub też nieświadomie, albo pod przymusem – ma odczucie, że wyimaginowana rzeczywistość, w którą wkracza, jest w stosunku do tej, w której na bieżąco żyje i działa, jej lepszą, bogatszą zmysłowo, atrakcyjniejszą poznawczo i emocjonalnie „wirtualną" reprezentacją.

Człowiek objęty doświadczeniem immersyjności nabywa przeświadczenia, że znajduje się w rzeczywistości, która *reprezentuje* tę, z której wyszedł, że jest ona jej znakiem, symbolem. Żyje zatem w nadrzędnej rzeczywistości, hiperrzeczywistości; na to właśnie wskazuje się w projekcie metawersum. Z teorii i badań nad zjawiskiem wielozmysłowego zanurzenia się w wyimaginowanym świecie wiemy, że na ogół ludzie doświadczający go są przekonani (wiedzą i mówią o tym), że są to *odmienne* rodzaje rzeczywistości; zazwyczaj nie mylą ich. Wiedzą, że jedna rzeczywistość zastępuje drugą. Dzięki temu dowiadują się czegoś więcej o rzeczywistym świecie, dokładniej rozumieją symulowane w ten sposób zjawiska (co ma miejsce w naukowych modelach złożonych zjawisk), w końcu też bawią się tą zwirtualizowaną rzeczywistością. W niej podejmują coraz więcej codziennych działań. I tutaj zaczynają się kontrowersje, z którymi projekt metawersum będzie miał do czynienia, gdyby miał być realizowany na skalę, o jakiej marzy Zuckerberg.

Jak działać w metawersie

Chodzi o to, co i *jak* ma robić człowiek immersyjnie wciągnięty w ten nowy wszechświat. Rzecz dotyczy istoty domniemanego *działania* w metawersum. Facebook deklaruje swój zamiar następująco: „Chcemy zabrać nasze społeczności w cyfrową przestrzeń, gdzie dochodzi do nowego rodzaju cyfrowej interakcji. (…) Nie chodzi o zastępowanie fizycznej obecności, nie chcemy, by ludzie spędzali więcej czasu online, chcemy by spędzali go za pomocą lepszej jakości interakcji" (wypowiedź Angeliki Gifford, wiceprezes Meta na Europę Środkową dla Polskiej Agencji Prasowej).

Zwykłe oglądanie, patrzenie i przeszukiwanie zasobów danych, właściwe dla zwyczajów wyniesionych z bezpośrednich, osobowych kontaktów, z rozmów, intelektualnego obcowania z książką i obrazem, chce się zastąpić „lepszą jakością cyfrowej interakcji". Jakiej jednak interakcji, należy spytać.

Z internetowych zapowiedzi, o infantylnym charakterze, wynika, że interakcje w metawersum mają być zapośredniczone przez awatary reprezentujące kontaktujących się użytkowników narzędzi oferowanych przez Facebooka i inne firmy. Ten nienowy pomysł implikuje jednak destrukcyjne konsekwencje dla relacji międzyludzkich, które miałyby powstawać na skutek takiego właśnie zwirtualizowania komunikacji międzyludzkiej. Dlaczego? Rzeczywiste działanie człowieka odbywa się na ogół w realnym środowisku, dotyczy konkretnych rzeczy i sytuacji, w konfrontacji z ludźmi, a nie ich reprezentacjami. Nawet jeśli wiele z czynów, rzeczy i aspektów osób, z którymi człowiek się spotyka, jest faktycznie mediatyzowane i zapośredniczone, to środki działania, jego cele i kryteria oceny są, mówiąc skrótowo, w realu, a nie wirtualu. Środki do działania w wirtualnej rzeczywistości znajdują się w realnym świecie, w nim też są kryteria ich doboru oraz oceny ich zastosowania. Dobre czy złe – skutki działania motywowanego najbardziej nawet fantazyjnymi, immersyjnymi treściami realizują się w świecie rzeczywistym.

> ***Chodzi o to, aby dać ludziom swobodę działania na niespotykaną dotychczas skalę, jednakże przy użyciu narzędzi i aplikacji firmy, która walczy o poszerzenie globalnego rynku swojej sprzedaży. Dotychczasową obecność w internetowej przestrzeni chce się zastąpić dogłębną immersją.***

Cała cywilizacja ludzka dowodzi tego stanu rzeczy. Humanitarne czyny przez stulecia warunkowane treściami Ewangelii, tak samo jak zbrodnicze działania podjęte po lekturze „Mein Kampf", były i zawsze będą udziałem realnych ludzi; są i będą oceniane ze względu na ich szlachetne lub złe, zawsze jednak fizyczne i realne skutki. Żadne z działań i współdziałań ludzkich podjętych w najbardziej nawet rozległym środowisku internetowym, a także ich praktyczne czy etyczne konsekwencje, nie realizują się wyłącznie w wirtualnym środowisku. Co do swej istoty są realnymi, a nie wirtualnymi czynami i wartościami; przeniesienie któregokolwiek z ich aspektów na poziom wirtualny nie czyni ich autonomicznymi. Awatar jest co najwyżej znakiem rozpoznawczym innego człowieka. To nie z nim, lecz drugim człowiekiem, z Innym wchodzimy we współdziałanie, porozumienie. Również tylko z Nim walczymy, jego tylko powiadamiany czy też oszukujemy. A jak miałoby być w metawersum?

Filozoficzne koncepcje, kognitywistyczne modele, empiryczne badania nie potwierdzają mrzonek facebookowego projektu. Działania oraz komunikowanie się, których

motywy, środki i cele mają źródła w realnym środowisku, nie rodzą trudności w interpretacji. Inaczej sprawa się przedstawia, gdy motyw działania oraz jego ocena miałyby być formułowane w wirtualnej rzeczywistości, zaś jego skutki dotyczyć tylko świata rzeczywistego. Gdy człowiek wyposażony w gogle dające mu symultaniczne wizje i modele świata, podejmuje praktyczne działanie (np. konstruuje maszynę) lub komunikuje się (rozmawia z bliskimi, uczy, poucza, ale i okłamuje), to motywy i skutki każdego z tych działań są oceniane w realnym świecie. Ocena ich treści czy wartości ze względu na wykreowane wizje, technologicznie i immersyjnie doświadczone, zmieniłaby sens i wartość takiego działania. W zasadzie podważałaby ich sens. „Rozmowa" z cudzym lub własnym awatarem, poleganie na „lepszej jakości cyfrowej interakcji" z anonimowymi interlokutorami czy wchodzenie w odpersonalizowane relacje ze „znajomymi" i „przyjaciółmi" – w tym wszystkim są wyłącznie pozorne i mylące motywy i treści działania. Jest to tylko gra między znakami i reprezentacjami działań i rzeczy, które już nawet nie udają, że cokolwiek reprezentują. Zauważył to kilka dekad temu, mając na uwadze telewizję, Jean Baudrillard w pracy „Symulakry i symulacja", twierdząc że w ramach takiej gry powstają samoistne symulakry – atrakcyjne symbole ukrywające brak swojego desygnatu i zachęcające ludzi do pozornych i destrukcyjnych działań. Symulakry choć są pełne nadmiarowej informacji, gdy występują w atrakcyjnej postaci obrazów oddziałujących na zmysły ich użytkowników, nie mają większej wartości i głębszego sensu. Udają, że mówią o rzeczywistości, podczas gdy oddalają od niej. – *Istniejemy we wszechświecie, w którym jest coraz więcej informacji, a coraz mniej sensu. (…) Informacja pożera własna treść. Pochłania komunikację i sferę społeczną. (…) Zamiast sprzyjać komunikowaniu, informacja wyczerpuje się w inscenizowaniu komunikacji* – pisał francuski filozof już w 1981 r. W metawersum mielibyśmy taką właśnie sytuację – wirtualna rzeczywistość i awatary zastąpiłyby codzienny świat doświadczenia i realnych ludzi.

Mityczne korzenie, religijne treści

Zarysowana powyżej sytuacja dwuznaczności działania wyłącznie w wirtualnej rzeczywistości wykazuje paradoksalnie cechy mistycznego doświadczenia religijnego. O wartości czynów człowieka decydować mają „pozaziemskie", „nie z tego świata" pochodzące cele i wartości. Mają się realizować w wyimaginowanym świecie wirtualnym, we wspólnocie jednakowo się zachowujących i doświadczających użytkowników informatycznych narzędzi oferowanych przez internetowego giganta.

Na specyficznie religijny charakter technologii informatycznych uwagę zwrócił już Erik Davis w monografii zatytułowanej *TechGnoza. Mit, magia + mistycyzm w wieku informacji*. Zauważył, że technologie komputerowe mają wręcz magiczną moc, gdyż nie tylko wytwarzają artefakty, jak chociażby wirtualną rzeczywistość, lecz również mity na ich temat, kształtują zwłaszcza fałszywy obraz człowieka i społeczeństwa na swój temat. – *Tworząc nowy interfejs pomiędzy naszym ja, innymi ludźmi i światem zewnętrznym, technologie mediów same stają się częścią naszego ja, innych ludzi i świata zewnętrznego* – pisał Davis kilka dekad temu.

Technologie informatyczne wprowadzają człowieka w nowe, ponadrealne światy, co prowadzi do znaczących konsekwencji światopoglądowych o mistycznym charakterze. Zwłaszcza wszechogarniająca komunikacja internetowa przyczyniła się do wytworzenia wśród jej użytkowników, w tym zagorzałych teoretyków i propagatorów, przekonania, że jest doskonałą wspólnotą całej ludzkości, w której znajdzie ona swoją realizację, a nawet zbawienie. – *Technologie komunikacji są zawsze* – podkreśla Erik Davis – *technologiami sacrum, po prostu dlatego, że idea i przeżywanie sacrum zawsze kształtują ludzką komunikację.*

Choć jest to dość kontrowersyjna opinia, można ją odnieść do projektu metawersum, który obiecuje immersyjne wejście każdego z jego użytkowników do domniemanej wspólnoty idealnej komunikacji. Obietnica nowej jakości doznań i pełnej interakcji ze wszystkimi, którzy zechcą tylko użyć gadżetów i aplikacji globalnych koncernów informatycznych, przypomina nadzieję na zbawienie człowieka i ludzkości pod warunkiem poddania się warunkom, które oferują ich prorocy. Miałoby to być w przypadku metawersum specyficzne „technologiczne zbawienie", osiągane poprzez wspólne i jednakowo zwirtualizowane doświadczenia. Wyimaginowana wspólnota, o której marzą właściciele i menadżerowie informatycznych gigantów, ukrywająca w atrakcyjnej postaci VR ich rzeczywiste interesy, stałaby się kolejny raz miejscem manipulacji działań i doświadczeń rzesz wyznawców, mówiąc wprost – kupujących, omamionych iluzjami nowych technologicznych proroków.

Jest doprawdy wiele argumentów i stosownych działań, aby krytycznie odnieść się do takich iluzji, a co najmniej je obnażyć.

Cyber(nie)bezpieczeństwo a kryptografia kwantowa

Deklaratywnie cyberbezpieczeństwo jest jednym z podstawowych celów przy budowaniu systemów teleinformatycznych. Praktycznie dominuje jednak podejście, w którym podstawowym priorytetem jest uruchomienie określonych funkcjonalności i ich płynne działanie, zaś bezpieczeństwo bywa przeszkodą w realizacji tego celu.

Mirosław Kutyłowski

profesor na Wydziale Informatyki i Telekomunikacji Politechniki Wrocławskiej, założyciel Katedry Podstaw Informatyki i badań z zakresu kryptografii na tej uczelni. Przez lata był związany z: Uniwersytetem Wrocławskim (gdzie otrzymał wszystkie stopnie naukowe), Uniwersytetem Technicznym w Darmstadt, Instytutem Heinza Nixdorfa na Uniwersytecie Paderborn. Profesor wizytujący na Uniwersytecie Xidian.

Zajmuje się głównie tematyką wrogiej kryptografii, obroną przed słabymi punktami technologii kryptograficznych oraz rozwiązaniami implementowanymi na elektronicznych dokumentach tożsamości.

Reakcją na zagrożenia czy poważne incydenty bezpieczeństwa jest często nie konkretne działanie, ale poszukiwanie *Wunderwaffe* – cudownych technologii, które mają zniwelować skutki naszych zaniedbań. W sensie praktycznym niewiele zmieniają wymagania typu *privacy-by-design*. Już samo wprowadzenie do regulacji prawnych typu RODO tego typu wymagań jest dowodem, że fundamentalne zasady ochrony danych mogą być ignorowane.

Z drugiej strony finansowanie prac nad technologiami, które mogą doprowadzić do lockdownu systemów teleinformatycznych, jest co najmniej niezrozumiałe. Do technologii tego typu należy z pewnością zaliczyć kryptoanalizę kwantową. Powodzenie prac nad konstrukcją komputera kwantowego realizującego łamanie systemów opartych na RSA i DLP w skali produkcyjnej doprowadziłoby do olbrzymich perturbacji w obrocie gospodarczym, załamania się ochrony wielu systemów i powrotu do papierowych mechanizmów obrotu sprzed kilkudziesięciu lat.

Błędy podstawowe

Obrona przed katastrofalnymi zagrożeniami dla systemów teleinformatycznych to nie tylko budowa rozwiązań typu *post-quantum*. W istocie popełniamy bardzo wiele błędów o charakterze strategicznym, zwiększających o rząd wielkości skalę zagrożeń. Dotyczy to nie tylko kryptoanalizy kwantowej, lecz również bardziej konwencjonalnych ataków. Warto dodać, że niekonwencjonalne metody prowadzenia obliczeń, odmienne od modelu von Neumanna, nie są zarezerwowane dla komputerów kwantowych. Szczególnie groźne mogłoby się okazać metody wtórnie wykorzystujące powszechnie dostępny hardware w niekonwencjonalny sposób. Nie należy wierzyć, że metody takie nie pojawią się nieoczekiwanie, tak samo jak kilkanaście lat temu pojawiły się nieoczekiwanie nowe jakościowo ataki na funkcje hashujące.

Błąd 1: centralizacja. Implementacja systemu informatycznego jest zwykle dużo łatwiejsza, gdy wszystkie komponenty systemu są centralnie i bezpośrednio sterowalne. Dotyczy to wszystkich faz cyklu życiowego – od projektowania, przez realizację i administrację, do rozmontowania systemu. Centralne zarządzanie w znakomity sposób ułatwia szybkie reagowanie na zagrożenia i systematyczne likwidowanie odkrytych podatności.

Ułatwienia stwarzane są niestety również dla atakującego: redukcji ulegają koszty wrogich operacji przy jednoczesnym wzroście efektywności. Nie sposób zapomnieć o asymetrii środków – obrona systemu zwykle bazuje na skromnych środkach finansowych, występują niedobory wykwalifikowanego personelu, często osoby te są przesuwane do zadań o wyższym priorytecie dla decydentów – takich jak wygoda systemu z punktu widzenia klienta. Po stronie atakującego ograniczeniem jest zwykle tylko wielkość potencjalnych profitów wynikających z przeprowadzenia ataku, zaś środki do ataku mogą być alokowane przeciwko dowolnemu systemowi w skali globalnej.

Problemu nie rozwiązuje tworzenie systemów mirrorów. Manipulacje danych dokonane przez atakującego mogą być automatycznie replikowane na systemy zapasowe. Problemu nie rozwiązuje również zabezpieczenie danych wykorzystujące mechanizmy blockchaina jako struktury istniejącej w pojedynczej fizycznej lokalizacji. Taki blockchain w niczym nie utrudnia zniszczenia danych przez atakującego.

Strategią, która niebywale utrudnia zaatakowanie systemu, jest jego rozproszenie i zaimplementowanie mechanizmów samostabilizacji i samonaprawy. Oczywiście, budowa takich systemów jest o rzędy wielkości trudniejsza pod względem koncepcyjnym, jednak w efekcie zainfekowanie nawet sporej frakcji komponentów nie prowadzi do załamania się systemu i utraty wiarygodności dokumentów cyfrowych. Przykładem podejścia tego typu jest koncepcja European Identity Wallet – europejskiej tożsamości cyfrowej. W rozwiązaniu tym odchodzi się od centralistycznych systemów, dostarczających wiarygodnych danych o tożsamości, na rzecz agregacji uwierzytelnionych informacji z różnych źródeł w portfelu użytkownika i pod jego kontrolą.

Błąd 2: brak planu B. Systemy informatyczne zazwyczaj są budowane i testowane pod kątem sytuacji standardowych. W tym zakresie bardzo niebezpieczna jest wiara w siłę rozwiązań kryptograficznych jako nienaruszalnych i niezmiennych w czasie. Perspektywę złamania algorytmów kryptograficznych, na przykład w kontekście metod kryptoanalizy kwantowej, traktuje się jako problem do rozwiązania w przyszłości, w przypadku pojawienia się takiej sytuacji. Niestety, wtedy będzie za późno i trudno będzie opanować powstały chaos.

Obawy należy mieć nie tylko ze względu na rozwój kryptoanalizy, w szczególności kwantowej. Przykładem krytycznego obszaru jest digitalizacja wielu kluczowych rejestrów danych i oparcie ich na standardowych systemach bazodanowych. Systemy takie niekoniecznie biorą pod uwagę niestandardowe zagrożenia, takie jak choćby możliwość fałszowania podpisów cyfrowych/pieczęci elektronicznych uwiarygadniających poszczególne wpisy (o ile w ogóle takie zabezpieczenia się wprowadza). W przypadku systemów takich jak księgi wieczyste, digitalizacja powinna być poprzedzona budową odpowiedniej infrastruktury typu *distributed ledger*, nie tylko uniemożliwiającej modyfikację już wprowadzonych rekordów (modyfikacja tylko w trybie append), lecz także pozwalającej na zrekonstruowanie rejestru z rozproszonych

części przechowywanych przez niezależnych uczestników. Wiarygodna rekonstrukcja powinna być możliwa nawet wtedy, gdy część uczestników jest nieuczciwa i pragnie zrekonstruować dane w nierzetelny sposób na swoją korzyść.

Jedną z zasad, która powinna obowiązywać w przypadku rozwiązań kryptograficznych, jest implementacja systemów automatycznie wykazujących, że system został skutecznie zaatakowany. Przykładem takiego pragmatycznego podejścia jest system podpisów elektronicznych realizowanych przez estońskie dokumenty tożsamości. Po pierwsze – rozproszono generowanie i użycie klucza podpisującego pomiędzy obywatela a serwer (plan B wobec groźby dostarczenia przez producenta kart kryptograficznych z zapadkami z jednej strony, a groźbą nieuczciwego wykorzystania podpisów serwerowych przez podmioty kontrolujące je – z drugiej strony), po drugie – zaimplementowano *nonces* w procesie generowania podpisu w taki sposób, by wykrywać nie tylko nieautoryzowane użycie, lecz także pojawienie się klonów elektronicznego dokumentu tożsamości.

Niewątpliwie hasła eliminacji gotówki z obrotu gospodarczego i oparcia obrotu finansowego na niewielkiej liczbie organizacji obsługujących rynek są krańcowym przykładem działania bez planu B, gdzie pojedyncze zdarzenie technologiczne (na przykład budowa efektywnych narzędzi podrabiania kodów MAC) może doprowadzić do załamania elektronicznej wymiany danych.

Błąd 3: tolerowanie produktów niebezpiecznych. Tak jak wiele innych nowoczesnych technologii, kryptografia, a w tym metody kwantowe, są nie tylko szansą, lecz także zagrożeniem. Kryptografia może chronić użytkownika, ale i w perfidny sposób służyć do atakowania go. Do użytku wszedł termin *malicious cryptography*, oznaczający wykorzystanie zaawansowanych metod nie tylko do zaatakowania, lecz także do skutecznego zamaskowania ataku. Niestety, mamy do czynienia z technikami, które w dowodliwy sposób zapewniają niewykrywalność – przynajmniej na poziomie klasycznej analizy inputu i outputu.

Kryptowaluty pozwalają na wolny obrót bardzo dużymi sumami i częstokroć zapewniają wysoki poziom anonimowości. Bez kryptowalut poziom zagrożenia atakami typu *ransomware* byłby zdecydowanie niższy, ze względu na trudności odebrania okupu w sposób bezpieczny dla przestępcy.

Wiele problemów wiąże się z używaniem narzędzi informatycznych w sposób nieodpowiadający istniejącym ryzykom z jednej strony, a własnościom narzędzi – z drugiej (na przykład smartfonów). W kontekście metod kryptograficznych istnieje tendencja do zastępowania twardej analizy bezpieczeństwa założeniami przyjmowanymi ad hoc. Dobrym przykładem jest sposób interpretacji norm FIPS 140-2 dla modułów kryptograficznych. Zamiast rozumienia ich jako *warunków koniecznych* (implementacja dobrych praktyk), posiadanie certyfikatu FIPS 140-2 bywa interpretowane jako *warunek wystarczający* dla zapewnienia bezpieczeństwa modułu i jego zastosowania.

> *Sztandarowym przykładem niekonsekwencji w działaniu jest z jednej strony zaostrzanie rygorów związanych z praniem brudnych pieniędzy, a z drugiej – tolerowanie rozwoju narzędzi znakomicie wspierających takie działania. Za przykład mogą posłużyć kryptowaluty.*

Catacrypt

Kilka lat temu powstał termin *catacrypt* jako skrót utworzony ze słów *katastrofa* i *kryptografia*. Nie brak opinii, że w istocie niekontrolowany i mało odpowiedzialny sposób budowy systemów informatycznych doprowadził do sytuacji, gdy w wielu obszarach istnieje sytuacja analogiczna do złamania podstawowych założeń kryptograficznych za sprawą powstania komputera kwantowego. Brak wykorzystania istniejących ścieżek ataku na szerszą skalę może być krokiem czysto taktycznym – nie zawsze istniejące możliwości wykorzystuje się natychmiast, ale czeka się na najbardziej odpowiedni moment. Jest to szczególnie ważne w przypadku zastosowań militarnych.

Zasada najsłabszego ogniwa łańcucha

Tak jak w każdej innej dziedzinie, obrona przed cyberatakiem powinna brać pod uwagę najsłabsze punkty systemu, a nie jego najmocniejsze strony. Niestety, w praktyce zbyt często upajamy się zaletami najbardziej dojrzałych komponentów, ignorując czasami fundamentalne słabości i nierozwiązane problemy innych składników tego samego systemu. Epatowanie zaletami najsilniejszych komponentów daje z jednej strony fałszywe poczucie bezpieczeństwa, a z drugiej strony jest cenną wskazówką dla atakującego, które scenariusze ataku są mało obiecujące i które komponenty atakujący powinien po prostu obejść, nie tracąc czasu na ich złamanie.

Dobrym przykładem jest skądinąd genialnie prosty protokół BB84 uzgadniania klucza drogą transmisji kwantowej. Przypomnijmy, że podstawową siłą tego schematu jest możliwość kwantowego przesyłania bitów w taki sposób, że atakujący *man-in-the-middle* przy próbie odczytu zmie-

nia wartość bitu z prawdopodobieństwem 0.25. Wynika to z faktu, że wysyłający i odbiorca, nazwijmy ich tradycyjnie Alicją i Bobem, wybierają przy przesłaniu każdego bitu jedną z dwóch baz do kodowania. Robią to niezależnie, bez jakiegokolwiek uzgadniania w tej fazie protokołu. W końcowej fazie do konstrukcji klucza sesyjnego brane będą tylko te bity, gdzie wybór bazy przez Alicję był taki sam jak wybór Boba. Z kolei, jeśli atakujący, nazwijmy go tradycyjnie Mallet, podsłuchuje komunikację, to aby odczytać wartość przesyłanego bitu, musi zdecydować się na jedną z baz. Jeśli wybierze inną bazę niż Alicja, to poprzez odczyt zmieni wartość przesyłanego bitu z prawdopodobieństwem 0.5. Tu kryje się pułapka na Malleta: w kolejnej fazie protokołu Alicja ujawnia Bobowi (już tradycyjnym kanałem) wybór bazy dla każdego bitu oraz wartości pewnej liczby bitów z losowo wybranych pozycji. Dzięki temu Bob może sprawdzić, czy ktoś po drodze nie zmienił wartości tych ujawnionych bitów poprzez błędny wybór bazy.

> *Tak więc BB84 nie jest w istocie protokołem uniemożliwiającym podsłuchiwanie komunikacji. Jest to protokół, który wykrywa podsłuch w kwantowym kanale komunikacji. Dzięki temu wydaje się, że omijamy wszystkie problemy występujące w klasycznej komunikacji radiowej, gdzie Mallet po prostu włącza odpowiedni odbiornik.*

Jak zwykle, diabeł tkwi w szczegółach i protokół BB84 jako taki nie stanowi wystarczającego zabezpieczenia. Najprostszy atak wiedzie poprzez urządzenie Alicji służące do generowania pomocniczych wartości losowych. Jeśli Mallet jest w stanie przewidzieć te wartości losowe, to cała argumentacja o wykrywaniu aktywności podsłuchującego wali się. Na przykład, gdy Mallet jest w stanie przewidzieć, które pozycje zostaną użyte do wykrycia podsłuchu, może po prostu nie ingerować w transmisję w tych momentach.

Jak widzimy, BB84 w krytyczny sposób zależy od generatora wartości losowych. Ten nie jest już związany w jakikolwiek sposób z mechanizmami kwantowymi i tym samym powracamy do starego problemu bezpieczeństwa klasycznych systemów informatycznych. Warto dodać, że nawet gdy odpowiedni generator jest zaszyty w bezpiecznym urządzeniu uniemożliwiającym infiltrację na drodze technicznej, to atakującym może być producent. Dzięki ujawnianiu dużej liczby wartości losowych w protokole BB84 bardzo łatwo jest zaimplementować podręcznikowy wyciek wewnętrznego stanu generatora metodami kleptograficznymi.

Jak widać, bezpieczeństwo uzgadniania klucza za pomocą protokołu Charlesa Bennetta i Gileada Brassarda wcale nie musi być wyższe niż w przypadku powszechnie stosowanego protokołu Diffie-Hellmana: oba są bezsilne, gdy generator wartości losowych Alicji został skutecznie zaatakowany. Tyle, że wykonanie protokołu Diffie-Hellmana prawie nic nie kosztuje…

Dokąd zmierzamy?

Na pewno konieczna jest koncentracja wysiłku na krytycznych obszarach i najbardziej pragmatycznych rozwiązaniach. Wymaga to, niestety, odważnego przedefiniowania priorytetów. Zarówno środowisko naukowe, przemysłowe, jak i działania podmiotów publicznych muszą przezwyciężyć swe przyzwyczajenia czy też partykularne interesy.

Dla przykładu, w środowisku naukowym badania są rozwijane bardzo często siłą inercji i podstawowym kryterium oceny jest poziom wyników, liczba punktów, cytowań itp., a niekoniecznie ich użyteczność.

Jakkolwiek systemy ewaluacji nauki zdają się zmieniać w dobrym kierunku, wiele jest w tym względzie do poprawy. Podobnie naturalnym procesem w sektorze gospodarczym jest maksymalizacja zysku, a niekiedy nawet dostarczanie produktów, które nie są trwale bezpieczne.

Cyberbezpieczeństwo po amerykańsku

Wbrew tytułowi artykuł nie dotyczy cyberbezpieczeństwa w USA. Przedstawia moją opinię na temat przydatności Narodowych Standardów Cyberbezpieczeństwa (NSC), przedstawianych jako zbiór rekomendacji standaryzujących rozwiązania zabezpieczające w sieciach i systemach informatycznych, wykorzystywanych przez podmioty chcące efektywnie zarządzać systemami bezpieczeństwa informacji.

NSC wprowadził Pełnomocnik Rządu ds. Cyberbezpieczeństwa z dniem 1 września 2021 r. w ramach realizacji interwencji 6.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 w zakresie opracowania i wdrożenia Narodowych Standardów Cyberbezpieczeństwa.

Z NSC można się zapoznać na stronie: https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber.

Made in USA

Jestem fanką amerykańskich standardów, wytycznych i dobrych praktyk dotyczących bezpieczeństwa informacji. Amerykanie w swoich opracowaniach piszą wprost, co warto zrobić i na co należy zwracać uwagę. Nawet Brytyjczycy czy Australijczycy (też Anglosasi) nie są tak bezpośredni.

Narodowe Standardy Cyberbezpieczeństwa to przetłumaczone wybrane publikacje National Institute of Standards and Technology (NIST), z których jako „godnych zaufania" korzystamy od lat. Należy jednak pamiętać, że są to standardy i wytyczne opracowane w celu zapewnienia wspólnego podejścia do problematyki bezpieczeństwa informacji i systemów teleinformatycznych **administracji federalnej USA**, której nie da się porównać

Joanna Karczewska
One of Europe's Top Cyber Women

z naszą administracją rządową i samorządową. Wprawdzie Departament Cyberbezpieczeństwa Kancelarii Prezesa Rady Ministrów zarzeka się, że standardy posiadają mapowanie na obowiązujące w naszym systemie prawnym Polskie Normy, ale samo mapowanie nie wystarczy, co pokażę na przykładach.

13 czy 17

Dyrektywa NIS wymaga od operatorów usług kluczowych i dostawców usług cyfrowych uwzględniania najnowszego stanu wiedzy w zakresie bezpieczeństwa sieci i systemów informatycznych. Popatrzmy na „Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013" (standard NSC 800-53 MAP wer. 1.0). Tu pojawia się pierwszy zgrzyt. Jak wynika z informacji umieszczonej na stronie Polskiego Komitetu Normalizacyjnego, odpowiednia polska norma PN-ISO/IEC 27001:2014-12 została wycofana i zastąpiona normą PN-ISO/IEC 27001: 2017-06. Dlaczego więc Narodowy Standard Cyberbezpieczeństwa wydany w 2021 r. nie uwzględnia zmiany normy dokonanej w 2017 r.?

Od lat uczestniczę w pracach nad metodyką COBIT i innymi dokumentami publikowanymi przez stowarzyszenie ISACA, którego jestem członkiem. Pamiętając jednakże o różnicach kulturowych i prawnych, staram się przekładać standardy amerykańskie na polskie realia. Stąd m.in. moje dwa uznane opracowania (nadal do znalezienia w Internecie):

- **wytyczna „UODO Survival Kit" z 2005 r., przygotowana razem z Mirosławem Błaszczakiem, Piotrem Dzwonkowskim i Sebastianem Łatasiem;**
- **„Mapowanie minimalnych wymagań dla systemów teleinformatycznych używanych przez podmioty realizujące zadania publiczne na COBIT 5" z 2013 r., przygotowane razem z Wojciechem Szyszką i Łukaszem Wilkoszem.**

Ukoronowaniem moich starań popularyzatorskich było wykorzystanie metodyki COBIT w trakcie kontroli „Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych", przeprowadzonej przez Najwyższą Izbę Kontroli w 2015 r. Miałam zaszczyt doradzać Izbie, jak za pomocą metodyki dokonać oceny poziomu zarządzania procesem „Zapewnienie bezpieczeństwa systemów informatycznych" w wybranych instytucjach administrujących systemami informatycznymi, służącymi do realizacji istotnych zadań publicznych.

Drugi zgrzyt dotyczy określenia „polityka", czyli angielskiego słowa „policy". Od lat posługujemy się pojęciem „polityka" w odniesieniu do regulacji wewnętrznych zatwierdzonych przez kierownictwo, zawierających opis podstawowych zasad oraz środków technicznych i organizacyjnych przyjętych w organizacji dla zapewnienia poufności, integralności i rozliczalności przetwarzanych informacji i danych osobowych. Norma PN-ISO/IEC 27001:2014-12 wręcz wymaga ustanowienia przez najwyższe kierownictwo **polityki** bezpieczeństwa informacji i komunikowania jej znaczenia. Dlatego nie rozumiem tłumaczenia „policies" jako „zasady" we wszystkich publikowanych NSC (z nielicznymi wyjątkami), chociaż w NSC 800-53 MAP zabezpieczenie „AC-1 POLITYKA I PROCEDURY" jest zestawione z punktem „5.2 Polityka" normy 27001.

Znowu od zera

Gdy zobaczyłam listę przetłumaczonych NSC, od razu pomyślałam – znowu zaczynamy od zera. Mamy odłożyć „stare zabawki" na rzecz nowych „przewodników metodycznych". Skoro tak, to należą nam się wyjaśnienia dotyczące kilku kluczowych kwestii:

1. **NSC 200 a Rozporządzenie o KRI**

   Czy NSC 200 wer. 2.0 „Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych" ma zastąpić rozporządzenie o KRI obowiązujące od 12 kwietnia 2012 r.? Zgodnie z rozporządzeniem, kierownictwo podmiotu publicznego jest zobowiązane do zapewnienia warunków umożliwiających realizację i egzekwowanie minimalnych wymagań dotyczących systemu zarządzania bezpieczeństwem informacji zawartych w § 20 ust. 2. NIK zdążyła już wielokrotnie zbadać stopień wdrożenia i stosowania tych wymagań. Jej raporty wskazują, że nadal nie jest najlepiej. Czy zatem NSC 200 ma być panaceum na trwające już 10 lat trudności w realizacji i egzekwowaniu bezpieczeństwa systemów informatycznych? Czy standard będzie lepiej „wspierać rozwój, wdrażanie i funkcjonowanie bezpieczniejszych systemów informatycznych"? Przydałoby się także wzajemne mapowanie obu zestawów minimalnych wymagań.

2. **NSC 800-37 a inne metodyki zarządzania ryzykiem**

   Czy NSC 800-37 „Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu" ma zastąpić wszelkie dotychczas opracowane i stosowane przez nas metodyki zarządzania ryzykiem? Są to m.in.:

   - „Metodyka zarządzania ryzykiem cyberprzestrzeni w systemach zarządzania bezpieczeństwem informacji podmiotów rządowych", opracowana przez Ministerstwo Administracji i Cyfryzacji i przyjęta w dniu 12 listopada 2015 r. przez Komitet Rady

Ministrów ds. Cyfryzacji, który rekomenduje administracji rządowej jej stosowanie;

- dwuczęściowy poradnik Prezesa Urzędu Ochrony Danych Osobowych zatytułowany „Jak rozumieć podejście oparte na ryzyku według RODO?" i „Jak stosować podejście oparte na ryzyku?", w którym przedstawione zostały kolejne możliwe etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz szczegółowej oceny ryzyka, czyli tzw. oceny skutków dla ochrony danych;

- „Analyse d'impact relative à la protection des données" (AIPD), opracowana przez francuski organ nadzorczy CNIL i przetłumaczona przeze mnie na język polski.

Przywołuję metodyki zarządzania ryzykiem dotyczące ochrony danych osobowych, ponieważ przetłumaczony NSC 800-37 wersja 2 z 2018 r. zawiera mnóstwo odniesień do prywatności oraz Personally Identifiable Information, w skrócie PII – po naszemu – do danych osobowych. Stanowi odpowiedź NIST na europejskie RODO. Tłumacze najwyraźniej nie wiedzieli o tym i na siłę uzupełnili standard o dopiski dotyczące danych osobowych, na dodatek zostawiając skrót PII w kilku miejscach.

3. NSC a szablony audytu zgodności z uksc

Czy nadal obowiązują opublikowane w kwietniu 2020 r. szablony sprawozdania z Audytu zgodnego z ustawą o Krajowym Systemie Cyberbezpieczeństwa? Czy szablony zostaną dopasowane do NSC? Czy obecnie wymagane przez uksc audyty bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej powinny obejmować badanie zgodności z Narodowymi Standardami Cyberbezpieczeństwa? Szablony zawierają dość ogólne odniesienia do zapisów normy PN-EN ISO/IEC 27001 w zakresie wymagań stawianych systemowi zarządzania bezpieczeństwem informacji. Można skorzystać z NSC 800-53 MAP, ale przydałyby się dodatkowe wyjaśnienia.

4. NSC a Diagnoza Cyberbezpieczeństwa

Czy zmianie ulegnie Formularz informacji związanych z przeprowadzeniem diagnozy cyberbezpieczeństwa JST? Diagnoza jest obligatoryjna dla rozliczenia grantu przyznanego w ramach programu Cyfrowa Gmina, ogłoszonego we wrześniu 2021 r. (po dacie publikacji NSC). Formularz obejmuje ocenę zgodności z rozporządzeniem o KRI i ustawą o ksc. Czy gminy powinny także sprawdzać zgodność z NSC 200?

Made in Poland

Tłumaczenie amerykańskiego tekstu technicznego jest równie trudne co przekład książek o Harrym Potterze. Na tłumaczy czyhają tysiące pułapek, nie tylko w postaci Dobby'ego/Zgredka. Błędne tłumaczenie może rozbawić specjalistę, a laika zwieść. Porównałam wersję amerykańską i polską standardu NSC 200 oraz NSC 800-61, który mnie szczególnie zainteresował, bo jako jedyny został dodatkowo zweryfikowany przez cyberbezpieczników. Oto co wykazała analiza:

1. Brak konsekwencji w adaptacji NSC do polskich realiów

Jak wynika z porównania, tłumacze pokusili się o różne modyfikacje, pominięcia i uzupełnienia, by „spolonizować" standardy. Niestety, nie byłam w stanie rozpracować, jaki przyjęli klucz. Nie rozumiem, dlaczego fragment o treści: *Advisories are often most necessary when new threats are emerging, such as a high-profile social or political event (e.g., celebrity wedding) that attackers are likely to leverage in their social engineering* zamieniono na: *Zalecenia są często najbardziej potrzebne, gdy pojawiają się nowe zagrożenia, takie jak ataki typu phishing np. z zainfekowanymi plikami pdf (pseudo faktury)*. Przecież u nas ataki z wykorzystaniem celebrytów czy wydarzeń politycznych też się zdarzają. Natomiast bez zmian pozostawiono scenariusz obsługi incydentu nr 3, który mnie wyjątkowo rozbawił.

Scenariusz obsługi incydentu nr 3: Skradzione dokumenty

W poniedziałek rano dział prawny organizacji odbiera telefon z organu ścigania w sprawie podejrzanej działalności związanej z systemami organizacji. Później tego samego dnia funkcjonariusz organu ścigania spotyka się z członkami zarządu i działem prawnym, aby omówić tę działalność. Organ ścigania prowadzi dochodzenie w sprawie publicznego opublikowania poufnych dokumentów rządowych, a niektóre dokumenty podobno należą do organizacji. Funkcjonariusz prosi organizację o wsparcie, a kierownictwo prosi zespół reagowania na incydenty o pomoc w uzyskaniu niezbędnych dowodów w celu ustalenia, czy te dokumenty są legalne, czy nie, oraz w jaki sposób mogły zostać ujawnione.

2. Brak znajomości amerykańskiego języka technicznego

Przy mechanicznym tłumaczeniu pojawiają się zabawne potworki językowe (ang. „gibberish"), np.:

- statement of management commitment – oświadczenie o zaangażowaniu w zarządzanie;

- images of clean OS and application installations – obrazy „czystego": systemu operacyjnego i instalacji aplikacji;

- hosts should have auditing enabled – hosty powinny mieć włączone przeprowadzanie audytu;
- affected external parties – dotknięte podmioty zewnętrzne;
- non-networked systems – systemy niezwiązane z siecią;
- real-time blacklists – czarne listy czasu rzeczywistego;
- well-connected employee – dobrze skomunikowany pracownik;
- specific impact information about incidents – szczegółowe informacje o wpływie na incydenty;
- organizational information systems – organizacyjne systemy informatyczne;
- monitor information system security alerts and advisories and take appropriate actions in response – monitorować ostrzeżenia i porady systemu informatycznego oraz w odpowiedzi na to podejmować odpowiednie działania.

3. **Brak znajomości pojęć dotyczących cyberbezpieczeństwa (i nie tylko) oraz brak spójności w stosowaniu przyjętych polskich odpowiedników**

   Nawet jeżeli pojęcie jest zawarte w NSC 7298 Słowniku kluczowych pojęć z zakresu cyberbezpieczeństwa, to nie oznacza, że polskie tłumaczenie jest właściwe. Dla przykładu:

   - controls – przetłumaczone jako środki/zabezpieczenia, nam znane są od lat jako mechanizmy kontrolne;
   - compromise (rzeczownik) – naruszenie (w Słowniku i tekście), złamanie, włamanie (w tekście);
   - compromise (czasownik) – zagrażać, złamać zabezpieczenia (w tekście);
   - compromised (przymiotnik) – naruszony, zagrożony, zaatakowany, którego dotyczy luka, zainfekowany (w tekście);
   - incident indicator – wskaźnik incydentu, który w Słowniku jest opisany jako oznaka, że incydent mógł wystąpić lub może aktualnie występować; zatem objaw, oznaka czy symptom byłyby właściwszym odpowiednikiem (szczególnie w kontekście incydentu);
   - policies – zasady, polityki, reguły (użyto wszystkich trzech słów w jednym dokumencie);
   - public affairs office – biuro spraw publicznych organizacji (chyba chodzi o rzecznika prasowego);
   - legal staff – personel prawny, dział prawny (zdecydowanie tylko to drugie).

Dobre rady Wujka Sama

NSC są pełne dobrych rad. Czy jesteśmy przygotowani na tak pragmatyczne podejście do zagadnień związanych z bezpieczeństwem informacji, systemów teleinformatycznych oraz ochrony prywatności? Oto kilka kolejnych przykładów z NSC 800-61:

1. W punkcie 3.1.1. jest zapis: *Sposoby zgłaszania incydentów, takie jak numery telefonów, adresy e-mail, formularze online i bezpieczne systemy komunikatorów internetowych, których użytkownicy mogą używać do zgłaszania podejrzanych incydentów. Co najmniej jeden mechanizm powinien umożliwiać anonimowe zgłaszanie incydentów.* Sprawdziłam strony https://www.gov.pl oraz https://www.amw.gdynia.pl/. Nie znalazłam zalecanego mechanizmu.

2. W punkcie 3.2.4. jest zalecenie ustanowienia zasad retencji dzienników. Jak zaznaczono: *Tworzenie i wdrażanie zasad retencji dzienników, które określają, jak długo należy przechowywać dane dzienniki, może być niezwykle pomocne w analizie, ponieważ starsze wpisy dziennika mogą wskazywać na aktywność rozpoznania lub wcześniejsze wystąpienia podobnych ataków*. Warto przypomnieć, że wymogi dotyczące przechowywania zapisów dzienników systemów (logów) są określone w § 21 ust. 4 Rozporządzenia o KRI.

3. W punkcie 3.2.4. jest także zalecenie utrzymywania synchronizacji zegarów wszystkich hostów. Warto zaznaczyć, że Główny Urząd Miar udostępnia poprzez Internet usługę umożliwiającą synchronizację czasu w systemach komputerowych z czasem urzędowym obowiązującym w Polsce. Serwery czasu znajdują się w Głównym Urzędzie Miar, w Laboratorium Czasu i Częstotliwości. Są one synchronizowane z państwowego wzorca jednostek miar czasu i częstotliwości. Usługa jest dostępna całodobowo i bezpłatnie. Sama z niej korzystam na moich komputerach.

4. W punkcie 2.4.3., dotyczącym personelu reagowania na incydent [sic!] (ang. *Incident Response Personnel*), zaleca się, by każdy członek zespołu miał dobre umiejętności rozwiązywania problemów i umiejętność krytycznego myślenia (ang. *critical thinking*). Przejrzałam aktualne oferty pracy dla cyberbezpieczników. Nie znalazłam żadnego ogłoszenia, które by wymagało od kandydata krytycznego myślenia.

Podsumowanie

Każdy zestaw dobrych praktyk, który pomoże w zapewnianiu cyberbezpieczeństwa, jest wyczekiwany i pożądany. Byłabym jednak ostrożna w twierdzeniu, że korzystając z Narodowych Standardów Cyberbezpieczeństwa można **STOSUNKOWO ŁATWO** zbudować system zarządzania bezpieczeństwem informacji i sprawować nad nim niezbędną kontrolę. Mamy takie przysłowie: Bez pracy nie ma kołaczy.

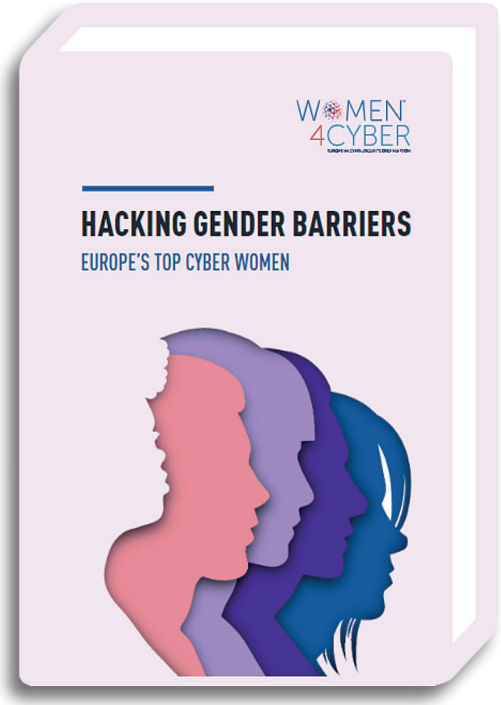
Na standardy NSC składają się następujące opracowania (materiały do pobrania na stronie https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber):

- Standardy kategoryzacji bezpieczeństwa (NSC 199 wer. 1.0)
- Minimalne wymagania bezpieczeństwa informacji i systemów informatycznych podmiotów publicznych (NSC 200 wer. 2.0)
- Przewodnik do opracowywania planów bezpieczeństwa systemów informatycznych w podmiotach publicznych (NSC 800-18 wer. 1.0)
- Poradnik Planowania Awaryjnego (NSC 800-34 wer. 1.0)
- Ramy zarządzania ryzykiem w organizacjach i systemach informatycznych. Bezpieczeństwo i ochrona prywatności w cyklu życia systemu (NSC 800-37 wer. 1.0)
- Przewodnik po telepracy w podmiocie publicznym (NSC 800-46 wer. 1.0)
- Zabezpieczenia i ochrona prywatności systemów informatycznych oraz organizacji (NSC 800-53 wer. 2.0)
- Zabezpieczenia bazowe systemów informatycznych oraz organizacji (NSC 800-53B wer. 1.0)
- Mapowanie środków bezpieczeństwa: NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013; PN-ISO/IEC 27001:2013 – NSC 800-53 wer. 2 (NSC 800-53 MAP wer. 1.0)
- Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część I (NSC 800-60 cz. 1 wer. 1.0)
- Wytyczne w zakresie określania kategorii bezpieczeństwa informacji i kategorii bezpieczeństwa systemu informatycznego część II (NSC 800-60 cz. 2 wer. 1.0)
- Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego (NSC-800-61 wer. 1.0)
- Architektura bezpieczeństwa systemów informatycznych w modelu „Zero zaufania" (NSC 800-207 wer. 1.0)
- Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa (NSC 7298 wer. 1.0)

Miałam rację

W dniu ochrony danych w 2018 r., na Stadionie Narodowym, w trakcie konferencji o znamiennym tytule „Zainwestuj w prywatność. Przygotowujemy się do RODO", spytałam przedstawicieli GIODO o prawa internautów, dotyczące ich danych zbieranych za pomocą narzędzia Google Analytics używanego na stronie GIODO. Odpowiedź była krótka i lakoniczna: mam sobie sama to wyjaśniać z Google. Cztery lata później, w dniu ochrony danych w 2022 r., sprawdziłam stronę UODO. Google Analytics już nie jest używane. Miałam rację, sygnalizując problem. Swoją drogą ciekawe, co się stało ze zgromadzonymi przez lata danymi o naszych wizytach na stronie urzędu.

Wszystkie informacje zawarte w artykule są podane według stanu na dzień 16 lutego 2022 r.



Cyberkobiety mają głos

Niedawno ukazała się publikacja „Hacking gender barriers: Europe's top cyber women" prezentująca sylwetki ponad 100 kobiet zajmujących się cyberbezpieczeństwem w Europie. Jej celem jest zaprezentowanie zarówno zróżnicowanych ról zawodowych pełnionych przez kobiety, jak i wielości dróg prowadzących do ich profesjonalnej aktywności w tej dziedzinie. Polskę reprezentują cztery specjalistki. Miło nam poinformować, że w tym wyróżnionym gronie znalazła się Joanna Karczewska, stała autorka tekstów o cyberbezpieczeństwie publikowanych na łamach Biuletynu PTI, a teraz – „Domeny".

Publikację wydała Women4Cyber – europejska fundacja non-profit, której celem jest promowanie, zachęcanie i wspieranie udziału kobiet w sektorze cyberbezpieczeństwa. Nie jest tajemnicą, że cierpi on na dotkliwy brak kadr, a udział kobiet w europejskim rynku pracy cyberbezpieczeństwa wynosi zaledwie 11 proc. – dotkliwie więc brakuje reprezentacji kobiet na wszystkich poziomach kompetencji. Women4Cyber, powołana do życie 3 lata temu przez ESCO (European Cyber Security Organisation), na różne sposoby stara się budować świadomość i promować dobre wzorce do naśladowania. Czyni to budując społeczność i upowszechniając jej osiągnięcia, wspierając programy edukacyjne, a także kształtując polityki na szczeblu unijnym i krajowym, zmierzające do podniesienia udziału kobiet w rynku pracy w obszarze cyberbezpieczeństwa.

Inspirujące success stories

Publikacja nie ma charakteru rankingu, to raczej próba pokazania, jak wiele dróg może prowadzić kobiety do takiego wyboru zawodowego i zachęcenia młodych kobiet do zainteresowania się taką ścieżką kariery. Każdej z bohaterek zadano te same pytania dotyczące obecnej pozycji zawodowej i jej związku z cyberbezpieczeństwem oraz pierwotnej ścieżki kariery i rad dla dziewczyn/kobiet chcących podążyć tą drogą. Poproszono również o wskazanie, co jest atrakcyjnego w pracy w cyberbezpieczeństwie i z jakich wzorów do naśladowania specjalistka korzystała. Można było także udzielić odpowiedzi na pytanie o tytuł inspirującej książki lub filmu.

Prezentowane specjalistki trafiły do cyberbezpieczeństwa z różnych branż, m.in. związanych z polityką klimatyczną, chemią, ale zdecydowana większość ukończyła kierunki informatyczne i ścisłe. Działają w dużych firmach informatycznych, bankach, firmach ubezpieczeniowych i konsultingowych, na uczelniach, a także w narodowych agencjach bezpieczeństwa. Są wśród nich zarówno właścicielki firm, jak i niezależne audytorki i ekspertki. Ta różnorodność karier i modeli działania robi wrażenie.

Na łamach publikacji nasz kraj reprezentują:

Izabela Albrycht
Politolog z wykształcenia. Współzałożycielka i przewodnicząca Komitetu Programowego funkcjonującego od 2014 r. Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC. Była prezes Instytutu Kościuszki, udzielająca się w licznych gremiach zajmujących się cyberbezpieczeństwem na szczeblu krajowym i światowym. Współzałożycielka Women4Cyber, w zarządzie DIGITAL EUROPE reprezentuje Polską Izbę Informatyki i Telekomunikacji, Związek Cyfrowa Polska oraz Krajową Izbę Gospodarczą Elektroniki i Telekomunikacji. W 2019 r. została uznana za jedną z 50 najbardziej wpływowych kobiet zajmujących się cyberbezpieczeństwem w Europie (Europe's 50 Most Influencial Women in Cybersecurity ranked by SC Media UK).

Joanna Karczewska
Absolwentka Wydziału Elektroniki Politechniki Warszawskiej. Ekspert ds. cyberbezpieczeństwa i ochrony danych osobowych z ponad 40-letnim doświadczeniem. Była wykładowcą na studiach podyplomowych Politechniki Warszawskiej i Akademii Marynarki Wojennej. Obecnie pracuje jako certyfikowany audytor systemów informatycznych i inspektor ochrony danych. Prowadzi szkolenia z zakresu audytu informatycznego i metodyki COBIT według autorskich programów. Aktywnie działa w międzynarodowym stowarzyszeniu ISACA jako Expert Reviewer metodyki COBIT5 i COBIT 2019 oraz publikacji dotyczących audytu informatycznego i GDPR/RODO. Ekspert Najwyższej Izby Kontroli.

Magdalena Skorupa
Wszechstronnie wykształcona – studia Executive MBA w HULT International Business School w Londynie; studia magisterskie o specjalizacji finanse-rachunkowość na Wydziale Zarządzania Uniwersytetu Warszawskiego; studia podyplomowe z górnictwa odkrywkowego na AGH w Krakowie oraz studia podyplomowe z psychologii społecznej w zarządzaniu zmianą w organizacji na SWPS w Warszawie. Posiada liczne certyfikaty (CISSP, CISM, ITIL Expert, PMP i wiele innych) oraz ukończone szkolenia branżowe zarówno z cyberbezpieczeństwa, jak i audytu wewnętrznego. Ekspert w dziedzinie bezpieczeństwa cybernetycznego, IT oraz zarządzania, ma ponad 20-letnie doświadczenie zdobyte w największych firmach na świecie. Specjalizuje się w projektowaniu, wdrażaniu oraz prowadzeniu programów podnoszenia świadomości cyberbezpieczeństwa w przedsiębiorstwach, prowadzi także własną firmę doradczą.

Joanna Świątkowska
Doktor nauk politycznych. Adiunkt naukowy na Akademii Górniczo-Hutniczej w Krakowie, pomysłodawczyni konferencji European Cybersecurity Forum – CYBERSEC. Senior Research Fellow Instytutu Kościuszki. Członek zespołu badawczego w Centre for Cybersecurity and International Relations Studies, University of Florence. Autorka licznych artykułów, raportów i analiz dotyczących cyberbezpieczeństwa. Często występuje na krajowych i międzynarodowych konferencjach i seminariach związanych z cyberbezpieczeństwem.

We see the pink colour

Europejska ekonomia, demokracja i losy społeczeństw coraz bardziej zależą od cyberbezpieczeństwa. Branża dramatycznie potrzebuje fachowców bez względu na płeć. Zasypywanie gender gap w tej dziedzinie pozwoli na budowanie bardziej zróżnicowanego ekosystemu cyberbezpieczeństwa, bo kobiety, wnosząc swoje doświadczenia i perspektywę w rozwój rozwiązań cyfrowych, przyczyniają się do wzrostu bezpieczeństwa cyberprzestrzeni. Celnie ujęła to Joanna Karczewska, pisząc, że: *kobiety są potrzebne, bo we see the pink colour, a zespoły ds. cyberbezpieczeństwa potrzebują różnorodności i różnych zestawów umiejętności, żeby móc skutecznie odpierać ataki*".

amk

W 2021 roku Komisja Europejska wraz z Women4Cyber uruchomiła pierwszy internetowy rejestr Europejek w dziedzinie cyberbezpieczeństwa. Baza danych The Women4Cyber Registry of Experts – ułatwiając współpracę grup ekspertów, przedsiębiorstw i decydentów z talentami w tej dziedzinie – ma pomagać w zaspokojeniu rosnącego zapotrzebowania na specjalistów ds. cyberbezpieczeństwa w Europie. To kolejny krok po uruchomieniu przed dwoma laty Europejskiego programu na rzecz zrównoważonej konkurencyjności.

Książkę można nabyć:
https://women4cyber.eu/roadmap-of-actions/100-women-in-cybersecurity-book

Secrets Chats Protocol

Nie istnieją obecnie uniwersalne mechanizmy ochrony danych o odpowiedniej jakości, które mogłyby łatwo zostać zintegrowane przez twórców aplikacji mobilnych. Opracowane rozwiązania są specyficzne dla danego systemu operacyjnego i najczęściej zależne bezpośrednio od jego wersji. Naszym celem było wytworzenie łatwego w implementacji, uniwersalnego systemu ochrony sekretów aplikacji składowanych w ramach jednego wspólnego kontenera.

Michał Glet

absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej (kierunek Informatyka, specjalność Kryptologia). Asystent badawczo-dydaktyczny w Instytucie Matematyki i Kryptologii WAT. Autor i współautor kilkunastu publikacji naukowych z zakresu kryptologii, cyberbezpieczeństwa oraz złośliwego oprogramowania. Twórca i współtwórca algorytmów i rozwiązań kryptograficznych oraz steganograficznych wyróżnianych na międzynarodowych wystawach wynalazczości. Ekspert w zakresie tworzenia i eksploatacji systemów informatycznych oraz rozwiązań z zakresu bezpieczeństwa, dostępności oraz poufności danych.

Kamil Kaczyński

absolwent Wydziału Cybernetyki Wojskowej Akademii Technicznej (kierunek Informatyka, specjalność Kryptologia). Asystent badawczo-dydaktyczny w Instytucie Matematyki i Kryptologii WAT, aktywny członek International Association for Cryptologic Research. Autor i współautor kilkunastu publikacji naukowych z zakresu kryptologii i steganografii. Twórca i współtwórca algorytmów i rozwiązań kryptograficznych oraz steganograficznych wyróżnianych na międzynarodowych wystawach wynalazczości. Ekspert w zakresie tworzenia i eksploatacji systemów zapewniających integrację z technologiami blockchain i mechanizmami kryptograficznymi pozwalającymi na zapewnienie poufności, integralności i dostępności danych.

Obecnie 3,5 mld użytkowników smartfonów korzysta z aplikacji, z których każda przechowuje potencjalnie wrażliwe dane. Aplikacje, które przetwarzają dane medyczne, finansowe lub osobiste (np. komunikatory mobilne) należą do grupy szczególnie zagrożonych i powinny być chronione z wykorzystaniem odpowiednio efektywnych metod. Tymczasem przykładowo niemalże 40% spraw rozwodowych, które mają miejsce we Włoszech, zawiera w materiałach dowodowych wiadomości wymieniane przez niewiernych małżonków za pośrednictwem aplikacji Whatsapp: http://www.thetimes.co.uk/tto/news/world/europe/article4262527.ece.

Wykorzystywany przez WhatsApp mechanizm ochrony danych nie jest więc wystarczająco bezpieczny, bo umożliwia łatwe odzyskanie historii prowadzonej komunikacji.

Podobne bolączki dotyczą aplikacji, których twórcy deklarują pełne skupienie na prywatności i bezpieczeństwie danych. Przed trzema laty wskazywaliśmy na luki bezpieczeństwa mechanizmu składowania danych Signal[1], który wykorzystuje jedynie mechanizmy systemu operacyjnego – w tym przypadku Android Keystore do przechowywania kluczy chroniących bazę danych. Ataki na mechanizm Keystore także były przedmiotem wielu publikacji naukowych ukazujących wpływ wykorzystania wybranych schematów kryptograficznych na bezpieczeństwo całego rozwiązania, w tym brak zachowania integralności szyfrogramu, co pozwala na zredukowanie długości wykorzystywanego klucza symetrycznego.

> *Należy także zwrócić uwagę, że mechanizmy systemu operacyjnego wiążą klucz główny urządzenia z wprowadzonym przez użytkownika sekretem – wzorem blokady, hasłem, kodem PIN, biometrią.*

Proces odzyskiwania sekretu może być przeprowadzony z wykorzystaniem oprogramowania śledczego, takiego jak Cellebrite UFED Ultimate, tym samym znacząco redukując poziom skomplikowania procesu odzyskiwania danych. W opracowaniu „Analysis of secure key storage solutions on Android"[2] autorzy dokonali analizy różnych metod bezpiecznego przechowywania kluczy, wskazując przy tym, iż na dzień opublikowania pracy żadna z badanych metod nie gwarantowała odpowiedniego poziomu ochrony. Większość z nich spełniała dwa z trzech wymagań – powiązanie z aplikacją, powiązanie z urządzeniem lub wymaganie świadomej zgody użytkownika na dostęp do danych. Powiązanie z aplikacją oznacza, iż dany sekret jest dostępny tylko dla wybranej instancji aplikacji, powiązanie z urządzeniem oznacza, iż sekret może być odczytany tylko przez dane urządzenie. Ostatnie wymaganie – świadomość użytkownika oznacza, iż klucz może zostać udostępniony jedynie wtedy, kiedy użytkownik wykona akcję potwierdzającą udostępnienie przechowywanego klucza kryptograficznego. W tej pracy zaproponowana została metoda, która pozwala na połączenie wszystkich trzech wymagań, tym samym stanowiąc rozwiązanie efektywne, także w przypadku występowania luk bezpieczeństwa mechanizmów systemowych.

Nasza propozycja

W celu ochrony sekretu aplikacji składowanych w ramach jednego wspólnego kontenera postanowiliśmy wykorzystać m.in. schemat podziału sekretu. Rozwiązanie takie jest zupełnie niezależne od wykorzystywanego systemu operacyjnego czy też zainstalowanych rozwiązań sprzętowych. Może być zatem z powodzeniem wykorzystywane na starszych urządzeniach. Stworzyliśmy uniwersalny mechanizm, który na bazie dostarczonego przez użytkownika hasła tworzy bezpieczny kontener dla przechowywanych danych. Rozwiązanie to może być wykorzystywane np. do ograniczania dostępu do zbiorów danych przechowywanych przez aplikację i z powodzeniem zastępować mechanizmy logiczne.

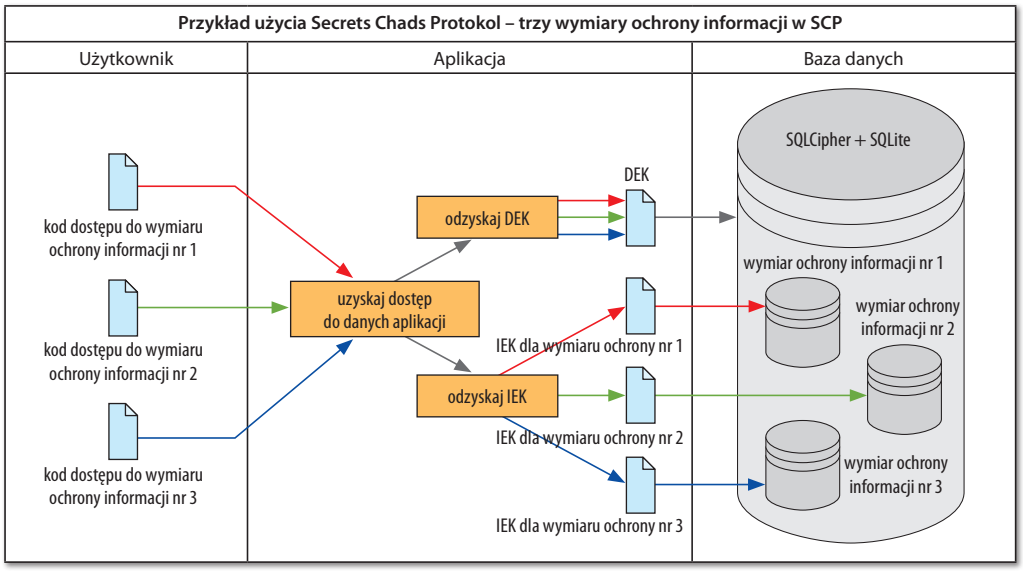
Na potrzeby opisu Secret Chats Protocol (SCP) wprowadzone zostały poniższe pojęcia:

- **Wymiar ochrony informacji** – zbiór danych, które podlegać będą ochronie i do których dostęp zostanie uzyskany za pomocą pojedynczego kodu bezpieczeństwa.
- **Database Encryption Key (DEK)** – sekret wspólny dla wszystkich wymiarów ochrony informacji.
- **Information Encryption Key (IEK)** – sekret unikalny dla każdego z wymiarów ochrony informacji.

1 K. Kaczyński, Security analysis of Signal Android database protection mechanisms. *International Journal on Information Technologies and Security*, Vol. 11, No 4 (2019), pp. 63-70.

M. Glet, Security analysis of Signal data storage mechanisms in iOS version. *International Journal on Information Technologies and Security*, Vol. 11, No 4 (2019), pp. 71-88.

2 T. Cooijmans, J. de Ruiter, E. Poll, Analysis of secure key storage solutions on Android. SPSM 2014: Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, pp. 11-20.



Architektura zakłada wykorzystanie hasła o wysokiej entropii, które jest krytyczne dla odpowiedniego poziomu bezpieczeństwa rozwiązania.

Kluczową częścią naszego unikatowego mechanizmu jest możliwość tworzenia wielu wymiarów ochrony informacji. Z punktu widzenia użytkownika, każdy wymiar wygląda jak oddzielna baza danych, bez możliwości dostępu do postaci jawnej danych innych wymiarów. Dostęp do danych danego wymiaru jest możliwy jedynie poprzez podanie poprawnego hasła zapewniającego dostęp do tego wymiaru – każdy wymiar posiada inne hasło dostępowe.

Idea jest bardzo prosta – rozwiązanie SCP ma umożliwić użytkownikom przechowywanie danych aplikacji w wielu wymiarach ochrony informacji. W danym momencie użytkownik uzyskuje dostęp do danych z pojedynczego wymiaru ochrony informacji. Co istotne, SCP nie ujawnia liczby wymiarów bezpieczeństwa, które zostały utworzone przez użytkownika.

W protokole SCP zakładamy, że jeden udział posiada zawsze aplikacja. Własności algorytmu Shamira sprawiają, że uzyskanie przez atakującego dostępu do tego udziału (np. poprzez analizę wsteczną kodu oraz danych aplikacji) nie wpływa na bezpieczeństwo sekretu. Drugi udział, niezbędny do odtworzenia wartości DEK, odzyskiwany jest z kodu dostępu wprowadzonego przez użytkownika. Mechanizm odzyskiwania DEK w SCP od klasycznej wersji algorytmu podziału sekretu Shamira odróżniają m.in. możliwości:

- stosowania dowolnych, wybranych przez użytkownika kodów dostępu;
- dynamicznego dodawania kolejnych udziałów (wymiarów ochrony informacji) bez konieczności modyfikacji już istniejących.

SCP wykorzystuje algorytm podziału sekretu Shamira[3] typu (2,k) (oznaczenie *SSS(2,k)*). Algorytm ten pozwala na ukrycie sekretu w *k* udziałach oraz odzyskanie go przy posiadaniu dowolnych *2* z nich. Pomysł Shamira bazuje na interpolacji wielomianowej oraz fakcie, że posiadając dowolne dwa punkty z przestrzeni R^2 (płaszczyzny euklidesowej) $(x_1,y_1),(x_2,y_2)$, takie, że $x_1 \neq x_2$, można skonstruować tylko i wyłącznie jeden wielomian $f(x) \in R[x]$ stopnia 1 taki, że $f(x_1)=y_1$ oraz $f(x_2)=y_2$.

Ten algorytm w SCP jest podstawą mechanizmu do odzyskiwania wartości DEK. W mechanizmie tym wykorzystujemy operacje w ciele GF(p) oraz wielomian postaci $f(x)=(a_0+a \cdot x) \pmod p$, gdzie *p* jest liczbą pierwszą. Wartość DEK jest ukrywana w wartości współczynnika $a_0=\tau(DEK)$. Secret Chats Protocol dzieli sekret na k części poprzez wyznaczenie współrzędnych punktów $(x_1,f(x_1))$, $(x_2,f(x_2))$,…, $(x_{(k-1)}, f(x_{(k-1)}))$, $(x_k,f(x_k))$. Posiadając dowolne dwa punkty, można odzyskać wielomian f(x) oraz wartość współczynnika a_0 i tym samym odzyskać wartość DEK.

Secret Chats Protocol dla każdego wymiaru ochrony informacji tworzy nowy udział w rozumieniu algorytmu podziału sekretu Shamira. W związku z tym instancja aplikacji posiadającej m wymiarów ochrony informacji wykorzystuje m+1 udziałów – jeden dla aplikacji oraz po jednym dla każdego wymiaru ochrony informacji. Dzięki temu, niezależnie od tego, która para udziałów zostanie wykorzystana (który kod dostępu zostanie użyty) do odtworzenia DEK, jego wartość zawsze będzie taka sama.

3 A. Shamir, How to share a secret. Communications of the ACM 22.11 (1979), pp. 612-613.

DEK

Zgodnie z tym, co zostało już przedstawione, wartość DEK (Database Encryption Key) jest taka sama dla każdego użytego kodu dostępu, czyli dla każdego wymiaru ochrony informacji. Jednym z założeń podczas tworzenia SCP było zapewnienie łatwej integracji z aktualnie istniejącymi aplikacjami. Część z nich, na potrzeby zabezpieczania składowanych danych, korzysta z szyfrowanych baz danych oraz rozwiązań typu SQLCipher. W tym przypadku wartość DEK może zostać wykorzystana do odzyskania klucza szyfrującego bazę danych. Rzeczywiste wykorzystanie DEK zależy tak naprawdę od twórców aplikacji. Prezentowany protokół SCP daje im sekret wspólny dla wszystkich wymiarów ochrony informacji, czyli dla wszystkich kodów dostępu zdefiniowanych np. przez użytkownika aplikacji.

Proces odzyskiwania DEK bazuje na algorytmie SSS(2,k) oraz autorskim algorytmie Common Container Algorithm (CCA). Wartość DEK ukrywana jest z wykorzystaniem algorytmu *SSS(2,k)*, natomiast algorytm *CCA* jest wykorzystywany m.in. do:

1. Zapewnienia użytkownikom możliwości stosowania własnych, dowolnych, kodów dostępu.
2. Przechowywania wszystkich danych związanych z *SSS(2,k)* w jednym miejscu.
3. Zapewniania możliwości łatwego składowania w istniejących aplikacjach.
4. Zapewnienia możliwości łatwego dodawania kolejnych wymiarów ochrony informacji, np. bez konieczności modyfikacji istniejących już wymiarów oraz kodów dostępu.

Szczegółowy opis kolejnych kroków algorytmu CCA oraz całego protokołu SCP można znaleźć w naszym artykule „Secret Sharing Scheme for Creating Multiple Secure Storage Dimensions for Mobile Applications”[4].

Co osiągnęliśmy?

Zaproponowany mechanizm ochrony danych pozwala na zwiększenie poziomu bezpieczeństwa danych aplikacji przechowywanych lokalnie. Pozwala on twórcom aplikacji na wykorzystanie zarówno mechanizmów dostarczanych przez system operacyjny, bezpiecznych modułów sprzętowych, jak i sekretu znanego tylko użytkownikowi. Dzięki tym założeniom użytkownik zawsze będzie musiał wyrazić zgodę na wykorzystanie kluczy kryptograficznych, co utrudnia wykonanie skutecznego ataku na dane aplikacji.

IEK

Secret Chats Protocol nie określa kroków ani procedur odtwarzania wartości IEK (Information Encryption Key). Wszystko zatem zależy od twórców aplikacji. SCP dostarcza aplikacji różne kody dostępu dla różnych wymiarów ochrony informacji. Na tej podstawie aplikacja powinna odzyskać np. klucze szyfrujące umożliwiające uzyskanie dostępu do danych przechowywanych w wybranym wymiarze ochrony informacji. W tym celu z powodzeniem można skorzystać np. z algorytmów opisanych w RFC-8018[5].

SCP definiuje także zupełnie nową jakość w dziedzinie ochrony danych przechowywanych we wspólnym kontenerze – pozwala na wykorzystanie wspólnej bazy danych, wewnątrz której istnieje możliwość wydzielenia dostępu do danych dla użytkowników znających sekret. Obecnie tego rodzaju ochrona jest realizowana z wykorzystaniem logiki aplikacji – dobrym przykładem jest tutaj komunikator Viber oraz jego funkcjonalność ukrytych czatów. Przy wykorzystaniu zaproponowanego rozwiązania możliwe jest tworzenie dowolnej liczby wymiarów ochrony informacji, bez ryzyka ujawnienia tej wartości np. poprzez analizę ustawień aplikacji. Rozwiązanie to może być szczególnie przydatne, gdy jedynie część historii prowadzonej komunikacji ma być prezentowana.

Jak SCP chroni przed Pegasusem?

W ostatnim czasie, m.in. w wyniku różnych medialnych doniesień, rośnie świadomość użytkowników związana z bezpieczeństwem oraz poufnością danych przechowywanych na urządzeniach mobilnych. Najczęściej omawianą oraz analizowaną publicznie aplikacją zagrażającą naszym danym oraz naszej prywatności jest Pegasus (P).

Pokusiliśmy się o estymację skuteczności SCP przy pewnych założeniach związanych ze sposobem działania oprogramowania szpiegującego – jej wyniki przedstawiamy w tabeli. Należy jednak pamiętać, że wykorzystanie potencjału Secrets Chats Protocol zależy od deweloperów oraz konkretnych aplikacji.

4 M. Glet, K. Kaczyński, Secret Sharing Scheme for Creating Multiple Secure Storage Dimensions for Mobile Applications. *International Journal on Information Technologies and Security*, Vol. 12, No 4 (2020), pp. 83-102.

5 *Moriarty, Kathleen, Burt Kaliski, and Andreas Rusch*. Pkcs# 5: Password-based cryptography specification version 2.1. Internet Engineering Task Force (IETF) (2017).

Pomysł na Secrets Chats Protocol opublikowaliśmy w 2020 r. Został doceniony m.in. przez społeczność badawczo-naukową, co przyniosło nam medale na targach wynalazczości:

1. **Złoty medal Prix Eiffel 2021 za „Secret Chats Protocol", mgr inż. Michał Glet, mgr inż. Kamil Kaczyński, Lyon, Francja;**
2. **Złoty medal Inova Croatia 2020 za „Secret Chats Protocol", nagroda specjalna MIIA, mgr inż. Michał Glet, mgr inż. Kamil Kaczyński, Zagrzeb, Chorwacja;**
3. **Złoty medal Intarg 2021 za „Secret Chats Protocol", mgr inż. Michał Glet, mgr inż. Kamil Kaczyński, Katowice, Polska;**
4. **Złoty medal Euroinvent 2021 za „Secret Chats Protocol", mgr inż. Michał Glet, mgr inż. Kamil Kaczyński, Bukareszt, Rumunia.**

Załóżmy zatem, że:
1. Secrets Chats Protocol zaimplementowany został w aplikacji A w sposób poprawny, a jego użycie jest zgodne z proponowanym przez nas podejściem (w pełni szyfrowana baza danych z wykorzystaniem DEK, szyfrowane dane w wymiarach ochrony informacji z wykorzystaniem IEK).
2. Na urządzeniu mobilnym zainstalowane zostało oprogramowanie szpiegujące P.

Rozpatrzmy następujące założenia co do korzystania z aplikacji A:
A1. Użytkownik nie korzystał z aplikacji A od momentu infekcji oprogramowaniem P.
A2. Użytkownik korzystał z niektórych wymiarów ochrony informacji w aplikacji A od momentu infekcji oprogramowaniem P.
A3. Użytkownik korzystał ze wszystkich wymiarów ochrony informacji w aplikacji A od momentu infekcji oprogramowaniem P.

Rozpatrzmy następujące założenia w kontekście oprogramowania szpiegującego P:
P1. Oprogramowanie P rejestruje w trybie ciągłym zawartość ekranu urządzenia mobilnego oraz aktywności interfejsu wejściowego (np. klawiatury ekranowej).
P2. Oprogramowanie P umożliwia utworzenie rzutu zawartości pamięci operacyjnej wszystkich procesów związanych z aplikacją A.
P3. Oprogramowanie P posiada dedykowaną funkcjonalność do analizy i monitorowania aktywności aplikacji A.

	A1	A2	A3
P1	Brak możliwości uzyskania dostępu do danych	Możliwość uzyskania dostępu do danych z niektórych wymiarów ochrony informacji, aczkolwiek wymaga (manualnej?) analizy zawartości nagranego ekranu oraz wprowadzanych danych	Możliwość uzyskania dostępu do danych ze wszystkich wymiarów ochrony informacji, aczkolwiek wymaga (manualnej?) analizy zawartości nagranego ekranu oraz wprowadzanych danych
P2	Brak możliwości uzyskania dostępu do danych	Możliwość uzyskania dostępu do danych z niektórych wymiarów ochrony informacji, aczkolwiek wymaga (manualnej?) analizy zawartości utworzonego zrzutu pamięci	Możliwość uzyskania dostępu do danych ze wszystkich wymiarów ochrony informacji, aczkolwiek wymaga (manualnej?) analizy zawartości utworzonego zrzutu pamięci
P3	Brak możliwości uzyskania dostępu do danych	Łatwa możliwość uzyskania dostępu do danych z niektórych wymiarów ochrony informacji	Łatwa możliwość uzyskania dostępu do danych ze wszystkich wymiarów ochrony informacji

Należy zaznaczyć, że:
1. „Brak możliwości uzyskania dostępu do danych" nie oznacza całkowitego bezpieczeństwa naszych danych. Nasze dane są tak bezpieczne jak bezpieczne są np. dane uwierzytelniające dostęp do nich, czyli wymiary ochrony informacji są tak bezpieczne jak bezpieczne są używane kody dostępu do nich (odpowiednia długość, zestaw używanych znaków itp.).
2. „Możliwość uzyskania dostępu do danych (...) aczkolwiek wymaga (manualnej?) analizy zawartości nagranego ekranu oraz wprowadzanych danych" oznacza, że operator oprogramowania P będzie musiał wykonać czasochłonną analizę uzyskanych danych (np. wideo z ekranem, logi z klawiatury), aby uzyskać dostęp do danych składowanych w aplikacji.
3. „Możliwość uzyskania dostępu do danych (...) aczkolwiek wymaga (manualnej?) analizy zawartości utworzonego zrzutu pamięci" oznacza, że operator oprogramowania P będzie musiał wykonać czasochłonną analizę uzyskanych danych (zrzuty pamięci), aby uzyskać dostęp do danych składowanych w różnych wymiarach ochrony informacji.

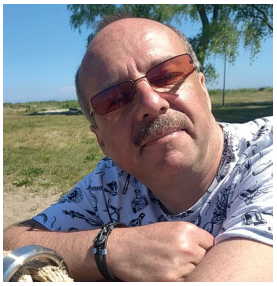
Warto podkreślić, że wszystkie czynności dotyczące oprogramowania P oraz aplikacji A, w których konieczna jest manualna aktywność operatora oprogramowania P, nie są odpowiednie do przeprowadzania inwigilacji na masową skalę.

Uczmy logicznego myślenia

O pomysłach na sensowne nauczanie informatyki w szkołach z Adamem Jurkiewiczem, autorem książki „Python 3" (recenzja na str. 50) i nauczycielem tego języka w liceum i technikum, rozmawia Tomasz Kulisiewicz.

Adam Jurkiewicz

zdobywca wyróżnienia Szerokiego Porozumienia na Rzecz Umiejętności Cyfrowych w Polsce w latach: 2017, 2020 i 2021, członek zarządu Szkolnej Sekcji Informatyki przy Polskim Towarzystwie Informatycznym. Autor książki „Python 3. Projekty dla początkujących i pasjonatów", wydanej przez Helion Edukacja, kursów języka Python dla projektu OSE IT-Szkoła – w zakresie szkoły podstawowej i szkoły ponadpodstawowej oraz współautor treści z języka Python w projekcie E-Podręczniki do kształcenia ogólnego dla klas ponadgimnazjalnych. Programista Python, administrator systemów UNIX/Linux, nauczyciel informatyki w pewnym liceum. Prywatnie – miłośnik szant, stateczny mąż, ojciec i dziadek, zwariowany nauczyciel młodzieży, jeśli tylko ma okazję.



Tomasz Kulisiewicz: Z grona 274 tys. maturzystów w 2020 r. informatykę rozszerzoną zdawało tylko niecałe 8,8 tys., podczas gdy matematykę rozszerzoną ok. 74 tys., fizykę rozszerzoną ok. 20 tys. Dlaczego informatyka na maturze – mimo braku informatyków na rynku i ich wręcz legendarnie wysokich zarobków – jest tak mało popularna?

Adam Jurkiewicz: Decyzje maturzystów są racjonalne. Egzamin z informatyki nie jest łatwy, a w zasadzie nic nie daje w staraniach o przyjęcie na studia, nawet na wydziały informatyczne. Brutalnie można powiedzieć, że nie opłaca się jej zdawać na maturze. Co z tym zrobić? A może niczego nie robić? Może tych kilka tysięcy maturzystów zdających informatykę rozszerzoną bez problemów dostaje się na studia informatyczne, a egzamin zdawali dla własnej satysfakcji i sprawdzenia się...

Mamy bardzo niski udział dziewcząt na wydziałach informatycznych. Na uczelniach wyższych kobiety stanowią większość, nawet na uczelniach technicznych jeszcze nie jest źle, ale wśród studentów i absolwentów wydziałów informatycznych kobiet jest zaledwie ok. 15%. Dlaczego? Czy da się przełamać tę tendencję?

Jeszcze do czwartej klasy szkoły podstawowej dziewczynki dają sobie radę z myśleniem algorytmicznym i „pre-informatyką", często lepiej od chłopców. Potem zaczynają działać stereotypy środowiskowe i nastawienia rodzinne: dziewczynom wmawia się, że są lepsze w kuchni, a w szkole – w przedmiotach humanistycznych czy artystycznych. Obawiam się, że w najbliższych kilku latach to się nie zmieni, ale może później. Na LinkedIn widzę coraz więcej kobiet w takich obszarach, jak webdevelopment czy projektowanie interfejsów, do czego potrzebne są zdolności plastyczne czy ogólnie coś, co tradycyjnie kojarzy się z kobiecymi umiejętnościami (np. rozróżnianie barw). Nie wiem, czy istnieją jakieś uwarunkowania psychofizyczne, może warto to badać. Wydaje mi się też, że kobiety lepiej odnajdują się w środowisku, lepiej współpracują w zespołach, dlatego więcej ich pojawi się w młodym pokoleniu ściśle współpracującym ze sobą w start-upach. Programowanie w tradycyjnym stylu jest chyba jedynym obszarem, w którym może działać „męski" model pracy samotnego nerda wklepującego po nocach kod do komputera.

Co Pana zdaniem zmienia tworzenie aplikacji narzędziami low-code/no-code? Za kilka lat będzie wokół nas 5 czy 10 razy tyle urządzeń IoT, ale na pewno nie będzie potrzeba do ich oprogramowania tyle samo razy więcej programistów. Jaka przyszłość czeka zawód informatyka?

Oczywiście narzędzia low-code/no-code umożliwiają działom biznesowym czy merytorycznym firm, urzędów i organizacji tworzenie aplikacji do wykonywania konkretnych zadań. Po odpowiednim przeszkoleniu można takie aplikacje składać z gotowych elementów i prawidłowo je parametryzować. Ktoś musi jednak zaprojektować, wykonać i przetestować takie narzędzia – choć i w tym obszarze już widać postępy automatyzacji. Na pewno idziemy w kierunku zmniejszenia udziału pracowitego wklepywania kodu, zamiast tego potrzeba będzie dużo więcej inwencji w opracowywaniu algorytmów, metod oraz narzędzi i bibliotek. Co do przyszłości zawodu: kiedy pojawiły się statki parowe, szkutnicy i budowniczowie pięknych żaglowców

czarno widzieli przyszłość zawodu. Jednak wraz z parowcami pojawiło się zapotrzebowanie na potrafiących je budować i naprawiać. Do kucia czy wypasu koni już nie trzeba tylu ludzi, ale kiedy pojawiły się konie mechaniczne, pojawił się zawód mechanika samochodowego. Telewizja miała spowodować bezrobocie wśród radiowców i filmowców, potem Internet miał wyrzucić na bruk specjalistów od telewizji. Oczywiście, były specjalności, które znikały, ale na ich miejsce pojawiały się dziesiątki nowych. Będziemy mieli do czynienia z zupełnie nowymi specjalnościami informatycznymi, których istnienia dziś nawet nie potrafimy sobie wyobrazić. Wystarczy spojrzeć, co się dzieje w uczeniu maszynowym i sztucznej inteligencji: pojawiają się trenerzy czy „pasterze" robotów. O przyszłość informatyków się nie obawiam. Zarządzać samokonfigurującymi się w zależności od warunków, wymagań itp. segmentami sieci 5G ręcznie się nie da, do tego potrzeba naprawdę sporo ML i AI, ale ktoś takie rozwiązania musi stworzyć, ktoś – kontrolować, czego i jak się uczą, dobierać dane do trenowania programów, ktoś musi umieć tuningować takie systemy.

To w takim razie warto postawić pytanie: czego uczyć w szkole – myślenia algorytmicznego czy programowania? I kto ma tego uczyć?

Na pewno trzeba wszystkich uczyć myślenia algorytmicznego, choć uważałbym na terminologię, bo nawet termin „algorytmika" z trudem przebija się wśród użytkowników TikToka i sam uważam, żeby nie przesadzać z taką terminologią wśród uczniów. Jak zwał, tak zwał – najważniejsze jest to, żeby uczyć wszystkich logicznego myślenia, również dlatego, żeby dorosłym ludziom nie dawało się wmówić wszystkich bzdur i kłamstw. Uczenie logicznego myślenia w dzisiejszej szkole jest trudne, a z punktu widzenia niektórych polityków – wręcz niekorzystne. Z drugiej strony jest też obecnie moda na uczenie wszystkich programowania. Nie wszystkim jest potrzebna umiejętność kodowania, ale wszystkim z pewnością przyda się zdolność logicznego myślenia. Dlatego to programowanie na poziomie do czwartej klasy szkoły podstawowej jest cenne, bo uczy właśnie myślenia logicznego, algorytmicznego, w dodatku na życiowych przykładach, np. porządkowania jakiś elementów otoczenia. Wchodzące trochę później środowisko Scratcha też jest przydatne jako wprowadzające różne abstrakcje w poglądowy i łatwy sposób.

Problem zaczyna się później, w klasach VII-VIII. Pomysł, żeby w tych klasach wprowadzić już tekstowy język programowania był dobry, pod warunkiem że będą potrafili tego uczyć odpowiednio wyszkoleni nauczyciele, a było z tym – delikatnie mówiąc – średnio. Dobrze o tym wiem, bo właśnie w tamtych latach uczyłem nauczycieli Pythona i zdawałem sobie sprawę, że trzeba im pomagać, bo dotąd na lekcjach informatyki uczyli głównie posługiwania się nieśmiertelnym programem do rysowania, czego zresztą mieli dość już i nauczyciele, i uczniowie.

Skąd wziąć nauczycieli do uczenia nowoczesnej informatyki? Nie pchają się do szkoły drzwiami i oknami. Trzeba by ich odpowiednio wynagradzać… Nie widać chęci do finansowego docenienia nauczycieli informatyki, tym bardziej, że od razu pojawi się pytanie: a dlaczego tylko nauczycieli informatyki? A co z pozostałymi?

Bardzo nam potrzeba uczenia wszystkich – i nauczycieli, i uczniów – stosowania narzędzi i rozwiązań informatycznych w różnych dziedzinach: w uczeniu polskiego, historii, biologii itp. Począwszy od prawidłowego korzystania z edytora tekstu, żeby coś napisać i żeby to dobrze wyglądało, miało prawidłową strukturę, dało się przetwarzać, nie mówiąc już o odczycie narzędziami dla osób niewidomych czy niedowidzących. W wielu szkołach ciągle jeszcze idzie się na lekcje informatyki do oddzielnej sali z komputerami, zamykanej kratą z dwoma kłódkami, bo jest tam kosztowny sprzęt, i walczy się ze smartfonami zamiast próbować ich wykorzystania w edukacji. Trochę to zmieniła pandemia, w społecznych inicjatywach powstawały serwisy takie, jak np. lekcjewsieci.pl, do których nauczyciele różnych przedmiotów wstawiają treści edukacyjne jako swoje pomysły na lekcje, wykorzystując powszechnie dostępne narzędzia informatyczne.

Od kilku lat zajmuje się Pan uczeniem Pythona, od niedawna w szkole. Nie wdając się w dyskusję „o wyższości świąt Wielkanocy nad świętami Bożego Narodzenia" – dlaczego Python i skąd uczenie w szkole?

Dobrze się złożyło, że właśnie wtedy, kiedy trzeba było zacząć uczyć tekstowego języka programowania, w podręcznikach pojawił się Python. To był dobry wybór, bo w odróżnieniu choćby od C++ Python ma „niski próg wejścia". A więc krótką odpowiedzią na pierwsze pytanie jest: bo Python jest łatwy, w dodatku łatwo się czyta programy – uczniowie przeważnie dają sobie radę z jęz. angielskim na tym poziomie i nie czują zniechęcenia zbyt wysokimi wymaganiami. Wprawdzie spotkałem się ze strony nauczycieli z pytaniami, dlaczego nie spolszczyć Pythona, by wszystkim było jeszcze łatwiej – ale pomińmy to milczeniem.

Na drugie pytanie odpowiedź też jest krótka: lubię uczyć ludzi, dzielić się swoją wiedzą. Poza tym poprosiła mnie o prowadzenie zajęć dyrektorka liceum, którą kiedyś uczyłem na kursach dla nauczycieli. Na szczęście na życie zarabiam w innych moich obszarach działalności, więc mogłem sobie pozwolić na wsparcie szkoły w bliskiej mi dziedzinie. Po latach prowadzenia szkoleń i kursów informatycznych dla dorosłych, w tym dla nauczycieli, skorzystałem z tej okazji, żeby wzbogacić swoje doświadczenie zawodowe. Uczę w liceum i technikum. Są to dla mnie bardzo ciekawe i ożywcze doświadczenia, dają wiele materiału do przemyśleń.

Eksperymentowałem w szkole z różnymi sztuczkami, na przykład pokazując na początku roku moim uczniom znany podręcznik „Black Hat Python"[1] – podręcznik hakowania, ale

tego, które nazywane jest *ethical hacking*, w odróżnieniu od przestępczego włamywania się do systemów – i pytając, kto chce zostać hakerem albo kto chce się nauczyć pisać boty do komunikatora Discord. Na początku prawie wszyscy z 300 uczniów zgłosili się tłumnie, myśląc, że za chwilę będą się potrafili włamywać do banków czy na strony rządowe. Zgodnie z założeniami kursu, do końca dotrwali tylko najwytrwalsi, którzy dali sobie radę ze sporym nakładem pracy, a przede wszystkim myślenia.

> ***A tak przy okazji – od dwudziestu lat walczę z zupełnie zniekształconym znaczeniem słowa „haker", oryginalnie opisującym kogoś, kto ma dużą wiedzę informatyczną i chce się nią dzielić. Choć to walka bardzo trudna, to jednak jeszcze się nie poddaję i na różnych konferencjach dla nauczycieli nie tylko przedstawiam się jako „haker edukacji", ale staram się to samo określenie podsuwać nauczycielom.***

Wracając do podstawy programowej – uważam, że czas byłoby zmienić podstawę dla liceum, która moim zdaniem ma za silny przechył w stronę pakietu Office. Dwadzieścia lat temu, kiedy wszyscy pracownicy biurowi musieli się nauczyć korzystania z komputerów, na pewno miało to sens, ale czasy się zmieniają. Uważam, że warto zajmować się w szkole TEXem. Ci, którzy się zetknęli z oprogramowaniem składu zbudowanym na systemie TEX wiedzą, że nie jest to zwykły program DTP, ale rozbudowany system programowania w języku znaczników. LaTEX i ogólnie TEX jest świetnym przykładem uczenia nie tylko składu, lecz także nauki specjalistycznego języka programowania, natomiast historia rozwoju tego systemu – przykładem tworzenia rozwiązań otwartoźródłowych: źródła od początku są w domenie publicznej. Pokazując LaTEXa swoim uczniom, mówię: zanim się przerazicie, że to takie skomplikowane, powinniście zdać sobie sprawę, że jeśli wybieracie się na dobre studia, na których będziecie musieli coś porządnie napisać, to na pewno się z nim spotkacie. Zapoznaję ich także z takimi edytorami, jak HackMD, edytor online bardzo popularnego, prostego i uniwersalnego języka znaczników Markdown, działającego w różnych środowiskach systemowych, stosowanego też w systemach zarządzania treścią.

Czy szkoła i uczelnia mogą nadążać za bardzo szybkim rozwojem metod i zastosowań informatyki?

Nie wdając się w rozważania na temat dzisiejszej polityki edukacyjnej i kierunków działań resortu edukacji i ograniczając do dziedziny, którą się bezpośrednio zajmuję: w szkole mamy do czynienia z kilkuletnim cyklem tworzenia i zatwierdzania podstawy programowej oraz podręczników – to w szybko rozwijających się dziedzinach stanowi dużą przeszkodę. Jeśli w fizyce stała grawitacji jest ciągle taka sama, choć i tam się wiele zmienia, to z informatyką mamy poważny problem wynikający z ogromnego tempa zmian. Problemem są też nauczyciele, którzy mają przekazywać tak dynamicznie zmieniającą się wiedzę. Czy szybkie zmiany da się przeprowadzić z obecną kadrą, czy też trzeba poczekać na wymianę pokoleniową? Z wymianą pokoleniową jest duży kłopot, bo jak wspomnieliśmy, nie widać tłumów młodych ludzi zgłaszających się do zawodu. Sytuacja zaczyna się robić podobna jak z pielęgniarkami: za kilka lat pójdą na emeryturę wszystkie, które nie są na tyle młode, żeby wyjechać do Niemiec, Szwecji czy Norwegii... W dodatku informatycy nie muszą się nawet ruszać z domu, żeby pracować na drugim końcu świata za duże pieniądze. Kto będzie uczył nauczycieli informatyki i ogólnie – informatyków – na uczelniach, na których młodzi nie chcą zostawać, a nawet kończyć drugiego stopnia studiów informatycznych? Ten problem wykracza poza ramy naszej rozmowy, powiem tylko, że od walki z wyimaginowanymi wrogami czy ideologiami ani PKB, ani Human Development Index czy inne wskaźniki rozwoju nam nie wzrosną. Na pewno potrzebna jest ogólnokrajowa dyskusja na temat modelu rozwoju kraju i rozwoju edukacji – a nie tylko rozwoju samej branży informatycznej. Trzeba przemyśleć, dokąd chcemy zmierzać.

Wracając do uczenia informatyki w szkołach: chętnie podyskutowałbym z resortem edukacji i z ekspertami nad „pływającą podstawą programową" informatyki czy nawet „dynamicznie samokonfigurującymi się programami nauczania", automatycznie dostosowującymi się do warunków i potrzeb, jak te sieci 5G, o których wcześniej wspomnieliśmy, „tuningowanymi" przez nauczyciela dobierającego elementy w zależności od umiejętności – i uczniów, i jego samego. Technicznie jest to możliwe do realizacji na przykład na platformach elektronicznych, do tworzenia takich programów nauczania można zastosować osiągnięcia ML i AI. Trzeba pokonać opór ludzi, którzy ciągle jeszcze nie mogą się przyzwyczaić do tego, że dziś i jutro jedyną stałą rzeczą wokół nas jest i będzie ciągła zmiana. Na razie takiego modelu uczenia, w którym nauczyciel sam sobie konfiguruje podstawę programową, nie da się zrealizować w dzisiejszym schemacie sprawdzalności zewnętrznej. Ogólnie realizacja takiego pomysłu w bismarckowskim modelu szkoły powszechnej jest niemożliwa, bo wymaga radykalnej zmiany sposobu myślenia o celach i metodach edukacji. To jest prawdziwe wyzwanie – i miejmy nadzieję, że zostanie kiedyś podjęte.

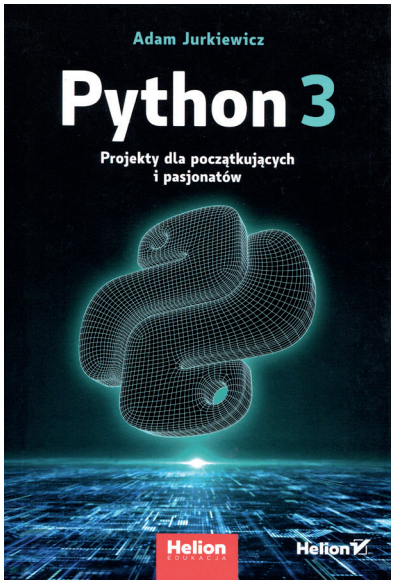
1 Autorstwa J. Seitza. Polskie wydanie „Black Hat Python. Język Python dla hakerów i pentesterów" (e-book, Helion, Gliwice, 2015).

Adam Jurkiewicz

Python 3

Projekty dla początkujących i pasjonatów

Helion, Gliwice, 2022



Wydana w tym roku książka „Python 3" Adama Jurkiewicza (rozmowa z autorem na str.?) jest czymś więcej niż tylko podręcznikiem języka programowania. Autor zakłada we wstępie, że młodzież – dla której przeznaczył swoją książkę – sięgnie po nią, bo chce ambitnie podejść do zdawania rozszerzonej matury z informatyki, bo słyszała, że programiści Pythona są cenieni na rynku pracy, czy dlatego, że chce zabłysnąć wśród koleżanek i kolegów. Zdaniem autora, każdy z tych powodów – łącznie z tymi, których nie potrafił odgadnąć – jest dostatecznie dobry .

Liczący niemal 80 stron rozdział pierwszy zawiera krótką instrukcję instalacji środowiska IDLE (Integrated Development Environment lub Integrated Development and Learning Environment) Pythona w środowisku linuksowej dystrybucji Mint 20 (z której korzysta autor), jak i w Windows. Autor wspomina też o środowisku IDLE dla macOS, a następnie omawia podstawy języka Python, podając proste przykłady kodu, w których zastosowane są omawiane elementy.

Kolejne rozdziały zawierają przykłady realizujące ideę autora: tworzenie programów dla konkretnych zjawisk i praktycznych zagadnień. Najpierw „oprogramowujemy" z autorem mechanikę ruchu: w rozdziale drugim autor przypomina „nieśmiertelną" grę Pong, powstałą równo pół wieku temu. Grę buduje, pokazując wykorzystanie biblioteki Pygame Zero służącej do tworzenia gier oraz grafiki z serwisu PixaBay do stworzenia tła, obrazu piłeczki oraz dwóch kresek-paletek, poruszających się tylko wzdłuż krawędzi stołu, jak w oryginalnej grze Pong na przystawki do telewizorów. Rozdział trzeci to wykorzystanie modułu *matplotlib* do tworzenia wykresu rzutu poziomego – klasycznego zadania mechaniki, w którym wprowadzane są dane o prędkości początkowej oraz wysokości, z jakiej rzucany jest obiekt. W rozdziale czwartym jest program wizualizujący mechanikę ruchu planet Układu Słonecznego na podstawie danych z serwisu NASA JPL Horizons pobieranych przy użycie modułu *astroquery*. Z przyczyn praktycznych program ograniczony jest do wizualizacji ruchu Merkurego, Wenus, Ziemi i Marsa, bo przy zachowaniu skali – jak żartobliwie wyjaśnia autor – do pokazania razem z tymi 4 planetami choćby tylko orbity Jowisza trzeba by mieć „baaardzoooo duuuuży monitor".

Rozdział piąty omawia pobranie i wizualizację na wykresie danych z portalu otwartych danych Urzędu Miasta Gdyni o statkach obsługiwanych w gdyńskim porcie i wizualizowanych z wykorzystaniem modułu *pandas*. W kolejnym rozdziale autor pokazuje na mapie Europy kilkanaście mniejszych polskich miast, korzystając z ich współrzędnych geograficznych zebranych w formacie CSV i umieszczanych na mapie przy wykorzystaniu modułów *matplotlib* oraz *cartopy*.

Ciekawe jest zadanie realizowane w rozdziale siódmym: usuwanie ze zdjęć szczegółowych metadanych EXIF zapisywanych w plikach przez cyfrowe aparaty fotograficzne. Dla zdjęć robionych telefonami komórkowymi zapisywane są nie tylko parametry aparatu (marka i typ, ustawienia przysłony, migawki oraz czas wykonania zdjęcia), lecz także współrzędne geograficzne GPS miejsca, w którym wykonywano zdjęcie. Zadanie to nie jest tylko zabawą, jeśli nie chcemy się dzielić tymi danymi z całym światem i zachować prywatność przy publikacji zdjęć w różnych serwisach. Zadanie to posłużyło autorowi do omówienia rekurencji.

W ostatnim rozdziale książki znajduje się porównanie wydajności Linuxa Mint 20 LTS oraz Windows 10 Home zainstalowanych „obok siebie" (w układzie dual boot) na tym samym komputerze. Porównanie to polega na zmierzeniu prędkości wykonywania w tych środowiskach programów napisanych w Pythonie: testu PyBench z otwartoźródłowego pakietu Phoronix Test Suite oraz skryptu stworzonego przez autora. Dla każdego przykładu prezentowanego w poszczególnych rozdziałach podany jest pełny kod programu, są też kody QR odsyłające do omawianych bibliotek i serwisów. Tekst ubarwiają autorskie uwagi, ostrzeżenia i wskazówki oraz krótkie cytaty z przeróżnych źródeł – od starożytnych mędrców i filozofów po postaci z naszych czasów. Książkę kończy apel autora do czytelników o kontynuację przygody z Pythonem.

Internet nie zapomina

Dzień Bezpiecznego Internetu (DBI), obchodzony z inicjatywy Komisji Europejskiej od 2004 r., ma na celu propagowanie działań na rzecz bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online oraz promocję pozytywnego wykorzystywania sieci. Zorganizowane z tej okazji przez Sekcję Informatyki Szkolnej webinarium: „Cyber(nie)bezpieczeństwa w edukacji" idealnie wpisało się w propagowane przez DBI działania.

Webinarium zgromadziło spore grono słuchaczy zainteresowanych zapowiadanymi odpowiedziami na wiele nurtujących nauczycieli pytań – począwszy od zagrożeń związanych z uwielbianą przez małoletnich aplikacją TikTok, poprzez problemy z niewłaściwymi treściami pojawiającymi się podczas pracy zdalnej po dostarczane do szkoły przez rodziców rachunki opiewające na kilka/kilkanaście tys. zł za zdalną edukację. Prowadzący webinarium Łukasz Gierek (patrz biogram) brawurowo odpowiedział na te i wiele innych pytań.

Prezentację rozpoczęła krótka sonda uliczna na podstawowy – wydawałoby się – temat: co to jest Internet? Odpowiedzi były zatrważające. – *Dostaliśmy Internet, ale bez instrukcji obsługi. Tymczasem świadomość tego, jaki ślad cyfrowy pozostawiamy w sieci jest kluczowa dla naszego bezpieczeństwa* – rozpoczął Łukasz Gierek (zainteresowanych prehistorią Internetu odsyłamy do artykułów autorstwa Jarosława Demineta w numerach 2 i 3/2021 Biuletynu PTI) https://portal.pti.org.pl/zasoby/biuletyn-pti/).

Łukasz Gierek

nauczyciel przedmiotów informatycznych w Zespole Szkół Technicznych w Radomiu. MIEExpert Microsoft Innovative Educator Expert, MIEFellow – Microsoft Innovative Educator Fellow, Skype Master Teacher. Wykładowca akademicki na Uniwersytecie Jana Kochanowskiego w Kielcach (kryminologia stosowana) i w Wyższej Szkole Handlowej w Radomiu (informatyka).

W tym roku Dzień Bezpiecznego Internetu obchodziliśmy 8 lutego. Zorganizowaną z tej okazji konferencję, adresowaną do przedstawicieli sektora edukacyjnego, organizacji pozarządowych i wszystkich osób zainteresowanych bezpieczeństwem dzieci i młodzieży w sieci, można obejrzeć: https://www.saferinternet.pl/dbi/transmisja-konferencji-dbi.html. W Polsce od 2005 r. organizatorem wydarzenia jest Polskie Centrum Programu Safer Internet, które tworzą Państwowy Instytut Badawczy NASK oraz Fundacja Dajemy Dzieciom Siłę – realizatorzy unijnego programu „Łącząc Europę" (ang. Connecting Europe Facility). Na stronie https://www.saferinternet.pl/dbi/pakiety-edukacyjne.html dostępne są pakiety edukacyjne dla dzieci, młodzieży i dorosłych. Wiele z nich można wykorzystać na lekcjach.

W wirtualnym świecie każde nasze zachowanie generuje cyfrowy ślad. Może on być pasywny, czyli dotyczyć danych użytkownika: na podstawie adresu IP – posiada go każdy komputer – można ustalić adres, pod którym znajduje się urządzenie, a także system operacyjny, zestaw zainstalowanych czcionek i ustawienia przeglądarek internetowych. Każde logowanie się do Internetu pozostawia ślad aktywny, bo cały ruch na komputerze użytkownika zostanie zapisany na serwerze dostawcy usług telekomunikacyjnych. Przeglądarki zapamiętują odwiedzane strony, wyszukiwarki – pytania, które użytkownik zadaje. Serwery za pomocą cookies śledzą aktywność użytkownika w sieci. Jeśli przy logowaniu gdziekolwiek podajemy dane osobowe, to nasz ślad cyfrowy zostaje z nimi połączony.

Co wie o nas Google?

Bardzo wiele. Zna nasze personalia, datę urodzenia, język, jakim się posługujemy. Dzięki coraz lepszemu rozpoznawaniu twarzy i tagowaniu w zdjęciach Google, wie, jak wyglądamy my i nasi znajomi. Każdy, kto ma pocztę na Gmailu, udostępnia Google nie tylko swoje maile, lecz także maile osób, z którymi koresponduje. Google wie, z kim rozmawiamy, bo widzi nasze kontakty w Gmailu, Google Hangouts i w telefonach z Androidem, w tym nazwiska, adresy e-mail i numery telefonów. Kalendarz Google podpowie, gdzie, kiedy i z kim się spotykamy. Każda nasza aktywność sprawia, że algorytm się uczy.

Google zna także tembr naszego głosu, bo jeśli mamy skonfigurowanego asystenta Google, to nas podsłuchuje. – *Przekonałem się o tym dobitnie, gdy wkrótce po rozmowie z żoną na temat bólu gardła w reklamach na moim komputerze pojawił się lek, który mi poleciła* – mówił Łukasz Gierek.

Śledząc historię wyszukiwania (Google Chrome rejestruje wszystkie odwiedzone strony internetowe lub zakładki, wszystkie filmy z YouTube, każdą kliknięta reklamę, a nawet liczbę automatycznych zapełnień przeglądarki), Google buduje nasz profil, obejmujący przekonania światopoglądowe, polityczne, gusty, preferencje, w tym seksualne. Jeśli próbujemy w sieci diagnozować chorobę, szukamy lekarza, apteki, domowych sposobów leczenia – to Google o tym wie. Gdy łączymy się przez Wi-Fi, GPS lub sieć komórkową, Google śledzi naszą lokalizację, a więc wie, gdzie i jak długo byliśmy.

Na https://timeline.google.com można wybrać dowolny, interesujący nas przedział czasowy i czerwone kropki pokażą miejsca naszego pobytu w wybranym okresie. Łukasz Gierek na przykładzie swojej wyprawy na Maltę w 2017 r. zademonstrował, jak dokładne mogą być informacje o naszym przemieszczaniu się. Po powrocie z Malty kilkakrotnie zmienił telefon, a mimo to po wejściu na stronę bez problemu odzyskał zdjęcia z tej wycieczki. Warto więc pamiętać, że dane GPS i zdjęcia przetrwają, mimo że zostały przez nas usunięte.

Gdy kończymy pracę w jakiejś firmie i nasze nazwisko znika z jej strony internetowej, nie oznacza to, że nie będzie można w przyszłości powiązać nas z tym miejscem pracy. – *To co trafi do Internetu, zostaje tam na zawsze* – mówił Łukasz Gierek, ilustrując swoją tezę pierwszą stroną Onetu z 1997 r., dostępną w Internet Archive. Roboty internetowe przeszukują i robią snapshoty wszystkich stron (z pełną funkcjonalnością można odtworzyć katalog, zdjęcia, muzykę).

Cyfrowych gadżetów przybywa i przybywa zagrożeń związanych z ich używaniem. Przykład – popularne opaski do treningów pokazują, gdzie biegamy, a analizując miejsce początku i końca treningu nietrudno ustalić, gdzie mieszkamy.

Gdy czytamy takie ostrzeżenia, nie robią na nas wielkiego wrażenia. Dlatego warto zobaczyć prezentowany na webinarium film, pokazujący, jak wiele można się o nas dowiedzieć tylko na podstawie naszego cyfrowego śladu: https://www.youtube.com/watch?v=CLRBYhd7e4Q.

– *Na postawie anonimowego zdjęcia w gazecie można zgromadzić całkiem pokaźną wiedzę o osobie na nim widniejącej: stan majątkowy, rodzinny, kredyt firmy, przy odrobinie szczęścia nawet numer paszportu* – ostrzegał Łukasz Gierek.

Uświadomieni są odporniejsi

Nikt nie powinien się łudzić, że wygra z cyfrowymi gigantami. Na początku tego roku Apple jako pierwsza spółka na świecie przekroczyła 3 bln dolarów giełdowej kapitalizacji. Nakłady Facebooka na badania i rozwój wyniosły w 2021 r. 20 mld dolarów. – *Meta Platforms stać na zbudowanie*

w jednym z najbiedniejszych krajów świata całej infrastruktury Internetu i dać każdemu mieszkańcowi kraju jedno z urządzeń (tablet, telefon, notebook) z dostępem do wyselekcjonowanych 35 stron tylko po to, żeby przeprowadzić eksperyment socjologiczny, jak zachowują się ludzie korzystający z sieci po raz pierwszy – mówił Łukasz Gierek. Na stronie https://justdeleteme.xyz można usunąć swoje konto z serwisów internetowych, ale z Facebookiem nie do końca się to udaje. Facebook Messenger jest nieusuwalny, dane pozostają na wieki. – *Gdy po jakimś czasie chcemy powrócić do używania skasowanego konta, budzi się ono z hibernacji – znów mamy swoje zdjęcie profilowe i grono znajomych* – zwracał uwagę prowadzący webinarium.

Zachowując elementarną ostrożność, możemy tylko nieco utrudnić proces pozyskiwania naszych danych i ich monetyzacji. Znajomość mechanizmów sieciowego biznesu pozwoli nam również z większą rezerwą odnosić się do proponowanych treści. Jeśli liczy się głównie czas naszego pobytu na jakiejś stronie, jej twórcy będą stosowali wszelkie chwyty, żeby nas zatrzymać. Stąd to morze bzdur, newsy cklickbaitowe, epatowanie sensacją. Rzetelność dziennikarska przestała być w cenie, weryfikacja przekazywanych informacji spoczywa więc na użytkownikach.

Sprawdź, co o tobie wiedzą

Do dyspozycji mamy OSINT (Online Source Intelligence), czyli grupę narzędzi do wyszukiwania informacji o swojej osobie. Na stronie https://haveibeenpwned.com/ można sprawdzić, czy nasze dane zostały naruszone przy okazji jakiegoś wycieku danych. – *Jeśli używacie tego samego adresu mailowego do logowania się na innych portalach i korzystacie z jednego hasła, to jeśli dane chociaż raz wyciekły, ktoś ma dostęp do wszystkich waszych serwisów, które macie podpięte pod to konto. Wchodząc w pocztę, można dotrzeć do konta bankowego, stąd do wyłudzeń tylko jeden krok* – ostrzegał Łukasz Gierek.

Nie bez przyczyny Łukasz Gierek rozpoczął swoją prezentację stwierdzeniem: *15 lat temu miałem włosy i nie miałem brody*. Zaprezentował zebranym, ile informacji dotyczących wykonanego przed 15 laty jego zdjęcia przetrwało (na stronie https://justdeleteme.xyz można to zweryfikować) – są to długie tabele danych, m.in.: autor, czas, miejsce, rodzaj sprzętu, przesłona, migawka, koordynaty twarzy, modyfikacje, kąt robienia zdjęcia, odległość aparatu od fotografowanego. To co trafi do Internetu, zostaje tam na zawsze. – *82 proc. amerykańskich rodziców udostępnia zdjęcia dzieci w sieci (w Polsce 43 proc.). Ba, 23 proc. dzieci zaczyna swój ślad cyfrowy zanim przyjdą na świat. Chodzi o zdjęcia USG, stanowiące źródło darmowych danych wrażliwych dla koncernów medycznych, których rodzice dobrowolnie by nie udostępnili. Większości użytkowników wydaje się, że dzielą się informacjami tylko ze swoimi przyjaciółmi i obserwatorami, ale tak nie jest. Wszystko, co udostępniamy w cyfrowym świecie, podąża za nami* – mówił Łukasz Gierek.

Czujność przede wszystkim

To zalecenie dotyczy przede wszystkim prawidłowego wykorzystania i niezbędnej aktualizacji narzędzi informatycznych. Teamsy nie aktualizują się same, należy zainstalować antywirusa na telefonie z systemem Android. Wtedy unikniemy wpadek w rodzaju tej, gdy za sprawą wirusa uczniowie na lekcji fizyki zobaczyli film pornograficzny. Nadal jednak nie powstały regulaminy, np. jak reagować, gdy uczeń nagrywa nauczyciela. Astronomiczne rachunki za nauczanie zdalne, przedstawiane przez niektórych rodziców, wzięły się z braku instrukcji, jak logować się do Teamsów, jeśli wybrano logowanie przez telefon, pojawiały się potężne opłaty roamingowe.

Czujność powinna też dotyczyć zachowań dzieci. – *Uważamy TikToka za super narzędzie do aktywizacji dzieci, tymczasem ich transmisje bywają naprawdę bulwersujące. Większość nagrań powstaje w domach i trudno uwierzyć, że do końca niepostrzeżenie. Warto też interesować się nagłym przypływem gotówki naszych pociech, galerianki przeniosły się do sieci i zarabiają camingiem* – radził prelegent.

Wielu słuchaczy webinarium pytało o możliwość zorganizowania szkoleń dla rad pedagogicznych. Łukasz Gierek zaoferował bezpłatne szkolenia dla szkół w województwach: pomorskim i małopolskim; warto, żeby z tych szkoleń skorzystali także rodzice (szczegóły i kontakt do prelegenta: https://sis.pti.org.pl/bezplatne-szkolenia-dla-rad-pedagogicznych).

Anna Kniaź

Przydatne strony do wykorzystania na zajęciach

https://thetruesize.com

https://www.internetlivestats.com/one-second/

Po co mi TIKi
czyli o „przezroczystości" technologii

Liczba bezpłatnych narzędzi TIK, jakie możemy wykorzystywać w szkole, rośnie lawinowo. Na jedno kliknięcie dostępne są generatory krzyżówek, rebusów, wykreślanek, zabawnych (lub ozdobnych) napisów, memów, gifów, quizów w dziesiątkach (a może i setkach) odsłon... Na wyciągnięcie myszki mamy platformy do tworzenia grafiki, prezentacji, filmów, animacji, komiksów, e-booków itd. Bardzo łatwo dzięki nim przygotować lekcję z tzw. efektem wow. Jeszcze łatwiej, niestety, zachłysnąć się kolejnymi poznawanymi narzędziami i na niemal każdej lekcji pokazywać uczniom kolejną, cudowną apkę. Niestety, blask taki może zamiast olśnić – oślepić.

Uczniowie po pierwszej fascynacji szybko poczują się zagubieni lub odniosą wrażenie, że uczą się przede wszystkim obsługi kolejnych narzędzi (wydaje się, że wraz z wprowadzeniem nauczania zdalnego w marcu 2020 r. wielu nauczycieli doświadczyło właśnie podobnego zagubienia przy kolejnych narzędziach prezentowanych na dziesiątkach webinarów). Co zatem zrobić, by korzystanie z apek (a szerzej z narzędzi TIK) było nie tylko efektowne, lecz przede wszystkim efektywne?

Kluczowa wydaje mi się przezroczystość technologii. Co mam na myśli? Poza lekcjami informatyki (gdzie sytuacja jednak trochę inaczej wygląda) wszystkie apki, platformy, generatory itp. powinny być niewidoczne, powinny stać się tym, czym w istocie swej są – NARZĘDZIAMI służącymi do realizacji celów. Nauczyciel, planując swoje działania, wie, jaki cel chce osiągnąć i jakie narzędzie (np. TIK) może mu w tym pomóc. Odwrotna kolejność myślenia (czyli: „poznałam nowe narzędzie i wyszukuję, w jaki sposób dopasować je do lekcji") bywa naprawdę zgubna.

Alicja Podstolec

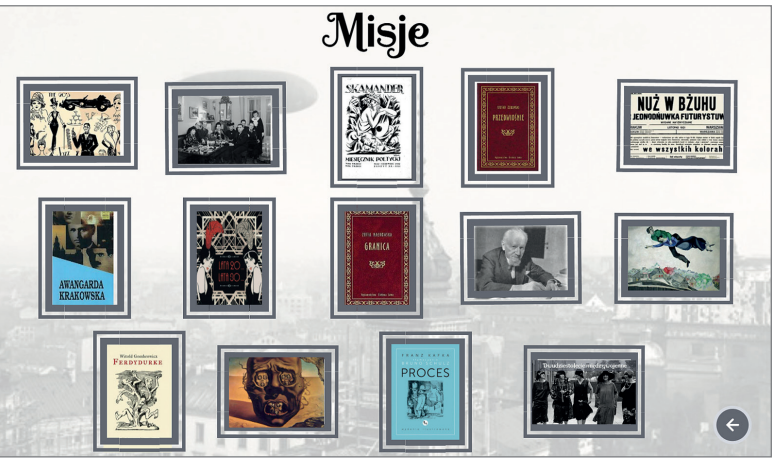
nauczycielka języka polskiego w Salezjańskim Zespole Szkół Publicznych im. św. Dominika Savio w Zabrzu oraz wykładowca języka migowego, autorka kilkunastu artykułów z zakresu dydaktyki oraz językoznawstwa, współredaktorka dwóch tomów serii „W świecie logopedii", współautorka e-booka „Turlane lekcje, czyli kostki na polskim. 20 pomysłów na niezwykłe lekcje języka polskiego", prowadzi blog https://nieprzecietne-lekcje.blogspot.com/. Ambasador Wakelet, Nearpod Certified Educator, Superbelfer RP

Narzędzia w grze

Taka „filozofia" korzystania z narzędzi TIK przyświecała mi, gdy budowałam zadania do zaprojektowanej przeze mnie gry edukacyjnej „Życie w wielkim mieście". Rozgrywałam ją przez ponad dwa miesiące z maturzystami. W ten sposób omówiliśmy całą epokę międzywojnia wraz z wszystkimi lekturami na 66 lekcjach (więcej o grze: https://nieprzecietnelekcje.blogspot.com/2021/11/co-to-bya-za-gra.html).

Trudność w przygotowaniu gry polegała m.in. na niepewności sytuacji – zaczynaliśmy rozgrywkę w szkole, ale wciąż

w powietrzu wisiało przejście na edukację zdalną (co zresztą się stało, uczniowie na 10 dni trafili na kwarantannę, szczęśliwie nie musieliśmy przerywać zmagań). Gra musiała być tak pomyślana, by można ją kontynuować również w sytuacji braku bezpośredniego kontaktu. Zdecydowałam więc, że podstawowym środowiskiem gry będzie prezentacja przygotowana w genial.ly.



Wybrałam tę platformę ze względu na łatwość przygotowania samej prezentacji, możliwość osadzania różnych zadań, wykorzystania adekwatnych do poszczególnych tematów grafik oraz sposób udostępnienia gry uczniom (przesłanie linku), a także możliwość rozbudowywania prezentacji w czasie trwania gry. Poza genial.ly korzystaliśmy z wielu aplikacji (m.in. Wakelet, Quizziz, AnswerGarden, Kahoot, Tricider, Canva, Nearpod, generator biletów), memów, wycinków z gazety). Czy to dużo? Być może, ale wszystkie one były podporządkowane zadaniom, a całość rozłożona w czasie. Przyjrzyjmy się kilku przykładom.

Uczniowie w pierwszym dniu gry otrzymali ode mnie imienne bilety wygenerowane tutaj: https://tickets.kadsoftwareusa.com/?fbclid=IwAR1lRJJZa7QcQUZSNef-B_I67N-Kv3__Qyvne-V-KMxQG5e5VAvn9zviCPkc.

Stały się one oczywiście początkiem fabuły, ładnym jej „materialnym" znakiem (w grze uczniowie przyjeżdżają z prowincji do Warszawy w roku 1918 i muszą się w stolicy odnaleźć).

To oczywiście trochę zbędny gadżet, właśnie po to, by uzyskać wspomniany efekt wow. To prawda, ale nie do końca. Na odwrocie biletów były bowiem kody QR, prowadzące do gry.

Było to o tyle istotne, że link do gry był oczywiście przesłany uczniom poprzez dziennik elektroniczny i grupę na portalu społecznościowym, ale zależało mi na tym, by uczniowie w czasie kolejnych lekcji mieli szybki dostęp do gry.

Wszystkie zadania obowiązkowe uczniowie wykonywali podczas zajęć w szkole. Dodam, że zasadniczo treść zadań nie odbiegała od tego, co robię z uczniami także poza grą. Zmienić się musiała czasem jedynie forma zadań w taki sposób, żebym mogła przyznać za ich wykonanie punkty. Czasem na przykład prosiłam uczniów o sformułowanie tezy interpretacyjnej jakiegoś utworu albo wskazanie w omawianym na lekcji tekście aluzji literackich czy też krótką interpretację plakatu z przedstawienia teatralnego. Zależało mi na tym, żeby wypowiedzieli się wszyscy uczniowie (po to, by zaktywizować całą klasę, a nie jedynie najbardziej zainteresowanych, a także dlatego, że zadanie miało być punktowane). W takich sytuacjach sięgaliśmy najczęściej po tzw. szybkie aktywności w aplikacji Nearpod. Pozwalają one na zadanie pytania otwartego lub utworzenie tablicy współpracy, gdzie uczniowie mogą przypiąć swoje odpowiedzi. Czy narzędzie TIK było tutaj konieczne? Oczywiście, że nie – w kilku podobnych sytuacjach uczniowie pisali swoje odpowiedzi na małych karteczkach, które mi oddawali. Efekt, można powiedzieć, taki sam. Ale znów nie do końca – gdy używaliśmy aplikacji zdecydowanie łatwiej było udostępnić uczniom odpowiedzi koleżanek i kolegów – a zatem przejść do kolejnego etapu lekcji – konfrontacji różnych opinii czy po prostu dyskusji nad zagadnieniem (dodam jeszcze, że łatwiej ocenia się zadanie, gdy ma się odpowiedzi zebrane w jednym linku niż na 28 kartkach).

Weryfikujące quizy

Omawianie niemal każdej lektury (a w grze były 4) rozpoczynam od jakiejś formy sprawdzenia stopnia przyswojenia przez uczniów jej treści. Naturalne więc było, że sięgnęli-

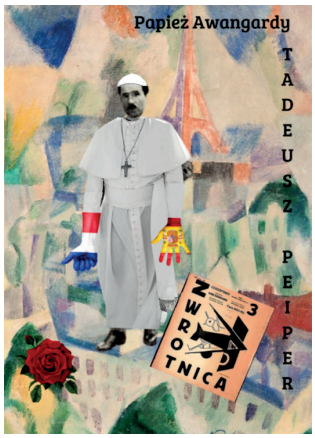
śmy tutaj po quizy – Quizziz i Kahoot (korzystam zasadniczo z tych dwóch narzędzi do tworzenia quizów – uczniowie je lubią, mają wszystkie potrzebne mi funkcje, nie mam więc potrzeby wyszukiwania kolejnych). Tutaj chciałabym jednak powiedzieć o nieco innym wykorzystaniu aplikacji. Otóż… jedno z ostatnich zadań dodatkowych (wykonywanych już poza lekcją, w domu) polegało właśnie na utworzeniu przez graczy quizu (miał być elementem lekcji powtórzeniowej). Nie muszę dodawać, że tworzenie quizu dla rówieśników pozwala na ćwiczenie przez ucznia innych umiejętności niż jego rozwiązywanie, a dodatkowo wymaga przypomnienia sobie wiadomości (w tym przypadku z epoki). Na zrobienie tego zadania zdecydowało się kilkoro uczniów, zagraliśmy więc w kilka różnych quizów z epoki międzywojnia. Było to o tyle ciekawym doświadczeniem, że mogliśmy zobaczyć, jak różne mogą być pytania, stało się to też przyczynkiem do dyskusji na temat tego, na jak różne kwestie zwracają uwagę tworzący testy.

Niektóre zadania dodatkowe wymagały od uczniów zajęcia stanowiska w jakieś sprawie (np. oceny różnych postaw poetyckich w międzywojniu) i wejście w polemikę z innymi uczestnikami rozmowy. Idealnym do takich aktywności narzędziem stał się Tricider. Uczniowie mogli odpowiadać na zadane przeze mnie pytanie dzięki linkowi podpiętemu do głównej gry. Od razu widzieli też odpowiedzi innych graczy i mogli się do nich ustosunkować.

W ramach zadań dodatkowych gracze mogli też np. tworzyć memy (do *Ferdydurke*) czy wycinki prasowe, jako relacje z rewolucji w Baku (*Przedwiośnie*), przygotowywali plakaty dotyczące biografii Peipera.


Kurier War
Wtorek, 22 marca, 1918 r.
Miasto rewolucji
Spokojne Baku zmieni o si w rozszala e miasto, którego mieszkańcy wyszli na ulice. Po pojawieniu si komisarza rewolucyjnego w sklepach zacz o brakowa towarów, a cz z nich zosta a nawet zamkni ta. Banki przesta y wyp aca pieni dze ludziom. Robotnicy przestali otrzymywa pensje i jakby tego by o ma o, ludzie wyrzucani s ze swoich mieszkań. Wielu z nich traci swoich najbliższych. Baku sta o si miejscem zbrodni i egzekucji, a konsekwencje tych wydarzeń b d ugo op akiwane przez mieszkańców.

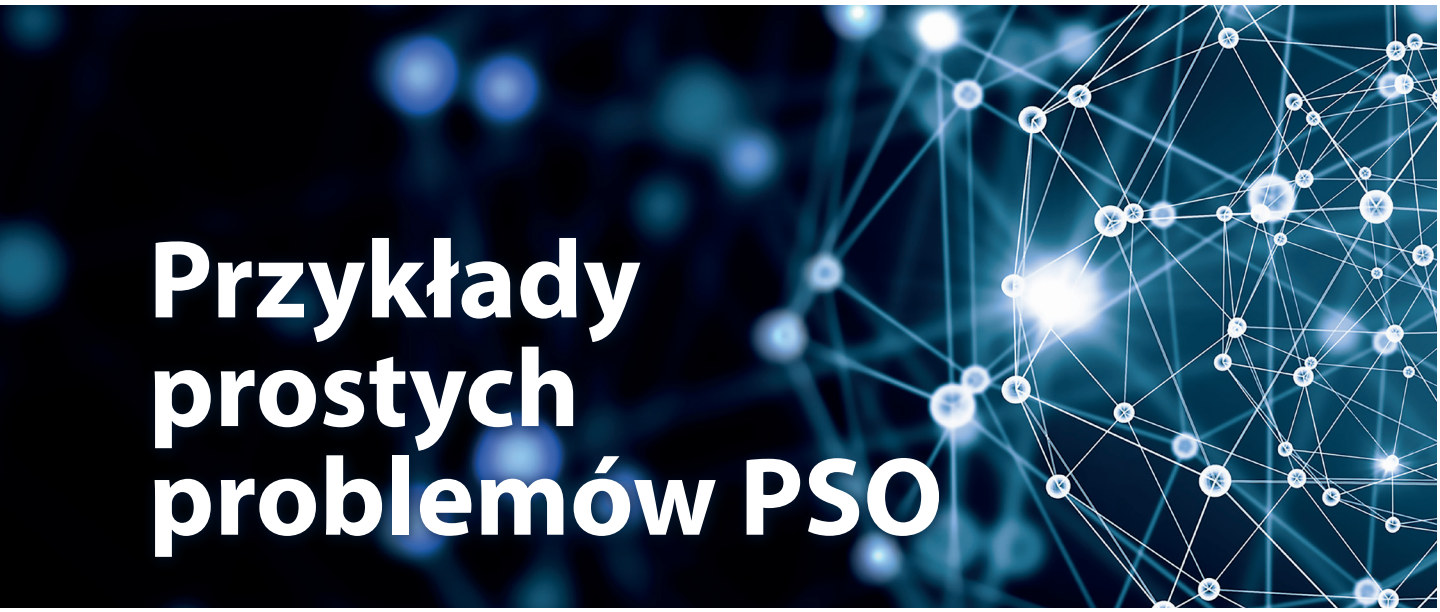
Korzystali tutaj ze znanych nam już wcześniej narzędzi, w tym ulubionej przez nich Canvy (w której przygotowałam też dla zwycięzców gry zaproszenia na bal). Wszystkie prace umieszczali na przygotowanych tematycznych Wakeletach. Dzięki temu uczniowie mogli zobaczyć nawzajem swoje prace (wiele razy zdarzało się, że się wzajemnie komplementowali), nie trzeba ich było nigdzie przesyłać, ryzykując zagubienie w poczcie elektronicznej, a ja po przyznaniu punktów oznaczałam pracę reakcją na Wakelecie, stąd nie było ryzyka, że coś pominę (zwłaszcza, że zadania te były długoterminowe).



Co istotne, wszystkie użyte w grze narzędzia były już uczniom znane (poznawaliśmy je stopniowo w ciągu poprzednich lat nauki), więc w czasie rozgrywki ich zastosowanie było dla wszystkich zupełnie oczywiste (nie zdarzyła się sytuacja, żeby trzeba było tłumaczyć sposób funkcjonowania narzędzia). Jeśli macie ochotę zobaczyć, jak wyglądała nasza rozgrywka, zapraszam tutaj (oczywiście usunięte zostały dane osobowe uczniów):

https://view.genial.ly/6148db426c5f750dd401c789/interactive-content-zycie-w-wielkim-miescie

Tekst jest rozszerzoną wersją artykułu opublikowanego na stronach Sekcji Informatyki Szkolnej PTI: https://sis.pti.org.pl/o-przezroczystosci-technologii/?fbclid=IwAR-0c0WnQeGlQGLo84YI1vHzZBV7sSQeo0p6qkCV9D-DwGDL2PU32aJ4Nu50I



Przykłady prostych problemów PSO

Przewodnik po nauczaniu informatyki kwantowej cz. 4.

Marek Perkowski

absolwent Wydziału Elektroniki Politechniki Warszawskiej, tu również zdobył tytuł doktora automatyki. Od 1983 r. pracuje na Wydziale Inżynierii Elektrycznej i Komputerowej w Portland State University, gdzie jest profesorem zwyczajnym i dyrektorem Laboratorium Robotów Inteligentnych.
Jeden ze współautorów WARP – pierwszego kompilatora języka VHDL dla układów FPGA. Twórca Diagramów Decyzyjnych Kroneckera, struktury krat logicznych i koncepcji robotów kwantowych. Przyczynił się do powstania oprogramowania dla syntezy logicznej, używanego w przemyśle USA. Pracował jako profesor wizytujący w Holandii, Francji, Japonii, Korei Południowej i Ludowej Republice Chin. W latach 2002–2004 był profesorem zwyczajnym w KAIST – Korean Advanced Institute of Science and Technology, gdzie zajmował się robotyką humanoidalną i komputerami kwantowymi. Kierował Komitetem Logiki Wielowartościowej IEEE w latach 2003–2005 i grupą roboczą Towarzystwa Inteligencji Obliczeniowej IEEE dla Inżynierii Kwantowej w latach 2006–2007. Autor ponad 515 publikacji o automatycznym projektowaniu, syntezie logicznej, logice wielowartościowej, logice odwracalnej, uczeniu maszynowym, robotyce i informatyce kwantowej.

Źródło: GetReal-WordPress.com

„Przewodnik po nauczaniu informatyki kwantowej" przedstawia metodologię rozwiązywania decyzyjnych Problemów ze Spełnianiem Ograniczeń (PSO) i problemów optymalizacyjnych z wykorzystaniem hybrydowego systemu komputera klasycznego i komputera kwantowego z algorytmem Grovera. Po wprowadzeniu układów odwracalnych jako rozszerzenia układów boolowskich pokazujemy superpozycję i splątanie kwantowe w sposób prosty, ale ścisły. Następnie przedstawiamy podstawowe dla wielu algorytmów kwantowych pojęcie wyroczni. Omawiamy, w jaki sposób wyrocznie są stosowane do rozwiązywania problemów decyzyjnych i optymalizacyjnych. Przykład znalezienia wszystkich „Optymalnych Zbiorów Suportujących" dla funkcji boolowskiej, który znajduje zastosowania w uczeniu maszynowym, dokładnie ilustruje proponowaną metodologię. Na koniec wyjaśniamy, jak działa algorytm Grovera. Po przeczytaniu tego cyklu uważny Czytelnik powinien być w stanie tworzyć podobne systemy kwantowe dla nowych, podobnych do przedstawionych, problemów.

Ponieważ problemy optymalizacyjne są redukowalne do Problemów ze Spełnianiem Ograniczeń (PSO), dlatego skoncentrujmy się na nich. PSO mają wiele zastosowań w syntezie logicznej, logice, kryptografii, robotyce, uczeniu się maszynowym czy sterowaniu.

Kolorowanie grafu

Dany jest graf G ze zbiorem węzłów N i zbiorem krawędzi E, krawędzie są parami węzłów $e_{ij} = (n_i, n_j)$. Węzły należy pokolorować funkcją KOLOR: N $\longrightarrow$ C, gdzie C jest zbiorem K kolorów. KOLOR (n_1) = *czerwony* oznacza pokolorowanie węzła n_1 kolorem *czerwonym*. Dla każdej krawędzi $e_{ij} = (n_i, n_j)$ musi być zachowane ograniczenie KOLOR $(n_i) \neq$ KOLOR (n_j), co oznacza, że każde dwa sąsiednie węzły muszą mieć różne kolory. Prawidłowe pokolorowanie grafu to takie, w którym to ograniczenie jest spełnione dla każdej krawędzi.

Należy znaleźć rozwiązanie dla następującego problemu decyzyjnego: *Czy jest możliwe pokolorowanie grafu G przy użyciu K kolorów? Jeśli tak, to pokaż to pokolorowanie. Graf jest K-kolorowalny, a liczba chromatyczna tego grafu jest K lub mniej.*

Algorytm PSO konstruktywnie znajduje: rozwiązanie tego problemu, więcej niż jedno rozwiązanie albo udowadnia, że problem ten nie ma rozwiązania. Użytkownik może łatwo zweryfikować, czy problem został dobrze rozwiązany. Choć znalezienie rozwiązania dla dużego problemu jest trudne, weryfikacja jest łatwa. Podkreślmy raz jeszcze, że powyższy problem jest problemem decyzyjnym, a nie optymalizacyjnym. Odpowiedzią na wszystkie problemy PSO jest albo „tak", albo „nie".

Sudoku

Wiele problemów można zredukować do problemu kolorowania grafu. Na przykład problem 4*4 Sudoku reprezentowany jest przez 16 kratek w macierzy 4*4, w której pewne kratki zawierają liczby 1, 2, 3, lub 4, a inne kratki są puste. Rozwiązanie polega na znalezieniu takich liczb ze zbioru {1, 2, 3, 4} dla pustych kratek w macierzy, żeby w każdym wierszu, w każdej kolumnie i w każdej z 4 narożnych 2*2 macierzy wszystkie liczby były różne.

Wyrocznię budujemy następująco. W kolorowaniu grafu dla każdej pary węzłów połączonych krawędzią komparator nierówności powinien dawać wartość 1 na swym wyjściu decyzyjnym, gdy na jego wejściach są różne kolory. Podobnie tworzymy graf układu wyroczni dla 4*4 Sudoku z 16 węzłami. Dla każdych dwóch węzłów z każdej kolumny umieszczamy w wyroczni komparator nierówności. Podobnie: dla każdych dwóch węzłów z każdego wiersza tworzymy komparator nierówności; dla każdego z czterech narożnych kwadratów 2*2 i dla każdej pary kratek w nich tworzymy komparator nierówności. Wyjście wielo-argumentowej bramki iloczynu logicznego I, której wejściami są wyjścia ze wszystkich komparatorów musi być = 1 dla każdego poprawnego rozwiązania problemu 4*4 Sudoku. Podobne wyrocznie łatwo jest utworzyć dla wielu znanych łamigłówek.

SAT

Innym problemem PSO jest słynny problem spełnialności (problem SAT). Dana jest formuła F w pewnej logice (na przykład boolowskiej). Pytamy: *czy ta formuła może być spełniona?* Co znaczy: *czy można znaleźć takie wartości jej zmiennych wejściowych, że F=1?* Na przykład, formuła $F(a,b) = (a+b) \cdot (a'+b) \cdot (a+b') \cdot (a'+b')$ w logice boolowskiej nie jest spełnialna. Formuła ta jest jednak 3-spełnialna, co znaczy, że jeśli usuniemy jeden z czterech termów sumacyjnych z powyższego iloczynu F(a,b), to formuła będzie spełnialna. Na przykład, formuła $F_1 (a,b) = (a+b) \cdot (a'+b) \cdot (a+b') = (a+bb') \cdot (a'+b) = a(a'+b) = ab$, zatem formuła jest spełnialna dla wartości wejść a=b=1. Taki problem nazywamy MAXSAT. Problemy SAT i MAXSAT mają setki zastosowań w praktycznych inżynierskich problemach, które są redukowalne do nich. Są to np. problemy optymalizacji układów cyfrowych czy analogowych, layoutu czy organizacji systemów sterowania. Również takie problemy, jak znajdowanie najlepszej drogi ewakuacji ludzi z terytorium katastrofy elektrowni atomowej. Problem spełnialności może być zredukowany do PSO. Podobnie problemy PSO mogą być zredukowane do SAT.

Problemy kryptoarytmetyczne

Jeszcze inny przykład problemu PSO to problem kryptoarytmetyczny: SEND+MORE=MONEY, w którym należy znaleźć podstawienie cyfr 0–9 za litery S,E,N,D,M,O,R,Y w jednoznaczny (jeden-na-jeden) sposób tak, by powyższe symboliczne równanie stało się prawidłowym równaniem na liczbach. Ta prosta łamigłówka jest maksymalnym uproszczeniem podobnych problemów w kryptografii, dziedzinie o ważnych zastosowaniach militarnych i komputerowego bezpieczeństwa. Podobnie do problemów SAT, kolorowania grafu czy innych problemów PSO, problem ten może być rozwiązany przez wyrocznię. Niekwantowe wyrocznie tego typu są budowane z bramek I, LUB, NIE, bloków logicznych takich, jak predykaty (A=B) lub (A>C) oraz bloków arytmetycznych takich, jak sumatory czy układy mnożące. Predykaty w naszym systemie logiczno-arytmetyczno-predykatowym są realizowane jako komparatory lub inne bloki biorące dowolne argumenty, ale zwracające wartości logiczne. Podobnie jak inne bloki, budujemy je z elementarnych bramek logicznych, stosując metody syntezy logicznej, specjalne metody i metody arytmetyki komputerowej.

Wszystko to pozostaje prawdą, gdy konstruujemy wyrocznię kwantową z bramek kwantowych. Metody konstrukcji są inne, ale podstawowa zasada zostaje ta sama. Umiejętność projektowania układów FPGA okazuje się bardzo przydatna dla programisty kwantowego. Inne omówienie problemów z wyroczniami można znaleźć w pracy Bshouty'ego i Jacksona[1].

Konstruowanie wyroczni jako kwantowych układów odwracalnych

Układy kwantowe są naturalnie odwracalne, zarówno poznane już układy permutacyjne, jak i dowolne układy opisane bramkami unitarnymi. Wynika to z własności macierzy unitarnych. Dla bramek „istotnie kwantowych" odwracalność ta istnieje w szerszym sensie – dla każdej macierzy unitarnej istnieje macierz odwrotna. Jest to wykorzystywane do budowania „układów zwierciadlanych", omówionych w następnej części. Istnieją również układy logicznie odwracalne, które nie zapewniają superpozycji i splątania, i nimi się nie zajmujemy. W tym tekście układy odwracalnych są układami kwantowymi.

Konstruowanie kwantowych układów odwracalnych jest podstawą konstrukcji wyroczni dla algorytmu Grovera. Ogólne wyrocznie w naszej metodologii są zależne od problemów i nawet od rozmiarów tych problemów. Algorytmy kwantowe to układy kwantowe budowane z bramek kwantowych, choć nie tylko z binarnych odwracalnych bramek kwantowych. Wyrocznia w algorytmie Grovera jest sercem tego algorytmu i jest zbudowana jedynie z bramek odwracalnych. Projektant nowych algorytmów bazujących na algorytmie Grovera pozostaje więc praktycznie w domenie boolowskiej. Inne bramki i bloki w tym algorytmie są niezależne od problemu, zawsze te same, łatwe do projektowania i dobrze znane. Nie ma potrzeby ich optymalizować. Użytkownik może znaleźć dla nich gotowe rozwiązania w języku QISKIT. Bramki Hadamarda na początku całego układu tworzą przestrzeń rozwiązań, a bramki Hadamarda łącznie z bramkami odwracalnymi służą do implementacji układów dyfuzji, które transformują krok po kroku niemierzalną informację z wyroczni do mierzalnej kwantowo informacji po szeregu powtórzeń pętli Grovera.

Zastosowanie algorytmu Grovera do nowego problemu to po prostu umiejętność sfomułowania tego problemu jako PSO, a następnie skonstruowanie układu kwantowego dla wyroczni i opisanie go w języku kwantowym. Dlatego zgrubny opis funkcjonalności tej ogólnej wyroczni może być wystarczający, a całościowy proces tworzenia programu dla algorytmu Grovera kompilowanego do poziomu realizowalnych bramek z pewnej biblioteki kwantowej – zaadaptowanego do naszego problemu – może być całkowicie zautomatyzowany. Systemów takich jeszcze nie ma, trwają nad nimi prace. Kiedy projektant-programista wie, jak zbudować wyrocznię w logice boolowskiej, to używając standardowych bloków arytmetycznych, może przetransformować swój abstrakcyjny opis do realizowalnych bramek odwracalnych – poprzez konwersję bramek boolowskich do bramek odwracalnych i użycie kwantowych bloków arytmetycznych, np. sumatora kwantowego z biblioteki takich bloków.

Metody translacji z logiki boolowskiej do odwracalnej są znane i w przyszłości zostaną w pełni zautomatyzowane. Przyszłe translator/symulatory języków kwantowych, podobnie jak obecne języki opisu sprzętu, takie jak System Verilog, będą wyposażone w bardzo złożone i inteligentne metody syntezy i optymalizacji na poziomie systemów, procesorów, bloków, układów i layoutu. Z punktu widzenia programisty będzie to jak przejście z poziomu programowania w assemblerze do poziomu programowania w PROLOGU.

Jak widzimy, wyrocznia to po prostu binarny układ kombinacyjny, a więc twórca wyroczni musi myśleć o swym problemie w terminach dekompozycji wszystkich abstrakcyjnych ograniczeń problemu PSO do poziomu znanych binarnych bloków i realizowalnych bramek. Funkcje odwracalne są matematycznymi odwzorowaniami (jeden-do-jednego) jednych binarnych wektorów w inne binarne wektory. Jeśli abstrakcyjna funkcja, którą chcemy zakodować w naszym układzie lub jego podukładzie, nie jest funkcją jeden-do-jednego, co zwykle ma miejsce, to ta funkcja nadal może być zmapowana do bramek odwracalnych, ale należy dodać tak zwane kubity dodatkowe (*ancilla qubits*). Problemem jest, że chcemy dodawać minimalną niezbędną liczbę takich kubitów, co jest związane ze sposobem kodowania naszego problemu do kubitów. Zwróćmy też uwagę, że większość funkcji boolowskich, używanych w typowych blokach arytmetycznych czy komparatorach w wyroczniach, nie jest odwracalna. Projektując bloki, musimy zrealizować je z kwantowych bramek odwracalnych. Oznacza to, że w każdym bloku musimy dodać pewną liczbę dodatkowych kubitów inicjalizowanych do stałych 0, aby móc zrealizować to odwzorowanie. Na przykład boolowski operator, dwuwejściowy iloczyn logiczny I(a, b) jest realizowany jako (A = a, B = b, C = ab $\oplus$ c) przy użyciu bramki Toffoliego z dodatkowym bitem c = 0. Zatem to, co nazywamy tutaj bramkami odwracalnymi czy blokami odwracalnymi, nie musi odpowiadać funkcjom odwracalnym w sensie matematycznym, gdyż w praktycznych

1 Bshouty, J., Jackson, J.: *Learning DNF over the uniform distribution using a quantum example Oracle*. Proceedings of the Eighth Annual Workshop on Computational Learning Theory, New York, 1995, s. 118–127.

wyroczniach wiele bloków nie jest matematycznie funkcjami odwracalnymi i posiada jeden lub więcej kubitów dodatkowych. Te bloki odpowiadają funkcjom boolowskim lub kodowanym binarnie dowolnym funkcjom niebędącymi odwzorowaniami jeden-do-jednego. Ten punkt często sprawia kłopot początkującym w językach kwantowych programistom. Jednak synteza takich bloków z dodatkowymi kubitami pozwala projektantowi posiadającemu doświadczenie w konstruowaniu klasycznych układów cyfrowych na natychmiastowe użycie swojej wiedzy i znajomości narzędzi projektowania EDA do budowania zoptymalizowanych i chytrych wyroczni kwantowych. Występują tu problemy znane z klasycznej syntezy układów cyfrowych i automatów, takie jak kodowanie[2] czy synteza w specyficznych bazach logicznych typu AND/EXOR czy – zwłaszcza – ESOP[3].

Należy mocno podkreślić, że idea realizowanej kwantowo wyroczni to znacznie więcej niż tylko wyrocznia Grovera. Można budować wyrocznię dla relacji (funkcji niezupełnie określonych). Można też projektować wyrocznie uogólnione, które poza wyjściem tak/nie i powtórzonymi wartościami zmiennych wejściowych dla rozwiązania, zwracają także inne dane, odpowiadające rozwiązaniom czy ich zbiorom, co może być przydatne do automatycznej konstrukcji następnych wyroczni kwantowych przez klasyczny komputer sterujący. Wyrocznie są więc układami cyfrowymi do rozwiązywania szerokiej klasy problemów odwrotnych.

Wielu autorów tworzy wyrocznie jedynie jako matematyczne koncepty, bez troski o ich praktyczną realizację z praktycznie realizowalnych bramek kwantowych. Zakładają oni, że każda macierz unitarna może być dekomponowana do jedno- i dwukubitowych macierzy unitarnych[4], co jest matematycznie prawdziwe, ale praktycznie bardzo trudne do policzenia. Na dodatek te wynikowe bramki mogą być nierealizowalne w praktycznym sprzęcie kwantowym. Dlatego propagowane tutaj podejście konstrukcji układów wyroczni „od dołu do góry" i to jedynie z bramek znanych i przebadanych jest bardziej praktyczne, choć czasem płacimy znaczną cenę – konieczność zastosowania dodatkowych kubitów.

Wymaganie realizowalności układów wyroczni jest bardzo ważne ze względu na dekoherencję, a także wtedy, gdy chcemy ocenić złożoność układu na podstawie liczby elementarnych bramek, a nie tylko na podstawie liczby ewaluacji układu wyroczni. Jak wiemy, algorytm Grovera daje kwadratowe przyspieszenie nad klasycznym algorytmem pełnego poszukiwania dla tego samego problemu, liczone w liczbie wywołań wyroczni. Ważne jest jednak, by brać pod uwagę nie tylko tę liczbę, lecz także czas i koszty układu poświęcone na jedno wywołanie wyroczni, na co pozwala przedstawiona metodologia.

Co możemy zrobić z algorytmem Grovera?

Fundamentalna idea algorytmu Grovera polega na znalezieniu rozwiązania dla Problemu Odwrotnego. Inne algorytmy kwantowe, np. algorytm faktoryzacji Shora, dają wykładnicze przyspieszenie, ale często mają ograniczone zastosowanie. Natomiast algorytm Grovera pozwala na zredukowanie do niego bardzo wielu praktycznych problemów typu PSO i optymalizacyjnych. Inne ważne algorytmy kwantowe, które mogą być przez nas użyte jako bloki czy podprogramy dla nowych algorytmów wysokiego poziomu, to algorytm estymacji fazy (phase estimation)[5], algorytm zliczania kwantowego (quantum counting)[6], algorytm szybkiej transformacji Fouriera, algorytm symulacji kwantowej i algorytm problemów algebry liniowej HHL (Harrow, Hasidim, Lloyd). Zwróćmy uwagę, że algorytm estymacji fazy używa algorytmu szybkiej transformacji Fouriera. Algorytm zliczania kwantowego wymaga algorytmu Grovera i algorytmu estymacji fazy. Algorytm Shora wymaga algorytmu szybkiej transformacji Fouriera i algorytmu estymacji fazy. Wiele algorytmów kwantowych sieci neurono-

2 Dhawan, S., Perkowski, M.: *Comparison of influence of two data-encoding methods for grover algorithm on quantum costs*. 41st IEEE International Symposium on Multiple-Valued Logic, 2011, s. 176–181; doi: 10.1109/ISMVL.2011.29.
Tsai, E., Perkowski, M.: A quantum algorithm for automata encoding. *Facta Universitatis, Series: Electronics and Energetics*, 2020, 33(2), s. 169–215.

3 Mishchenko, A., Perkowski, M.: Fast heuristic minimization of exclusive sums-of-products. Reed Muller 2001, Workshop.

4 Vartiainen, J.J., Möttönen, M., Salomaa, M.M.: Efficient decomposition of quantum gates. Phys. Rev. Lett. 2004, 92, 177902.
Khan, F., Perkowski, M.: *Synthesis of Ternary Quantum Logic Circuits by Decomposition.* Proceedings of 7th International Symposium on Representations and Methodology of Future Computing Technologies, RM 2005, s. 114–118.

5 Nielsen, M., Chuang, I.: *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

6 Brassard, G., Høyer, P., Tapp, A.: Quantum counting. W: K.G. Larsen, S. Skyum, G. Winskel (red.), *Automata, Languages and Programming* (s. 820–831). Berlin, Heidelberg 1998; doi: 10.1007/BFb0055105.

wej wymaga algorytmu Grovera. W konkluzji – wiele ciekawych nowych algorytmów kwantowych możemy utworzyć za pomocą jedynie algorytmu Grovera. Jeśli jednak dodatkowo zrozumiemy algorytm szybkiej transformacji Fouriera i algorytm estymacji fazy, a także algorytm symulacji kwantowej, to otwierają się przed nami duże możliwości tworzenia algorytmów kwantowych dla nowych problemów.

Wiele użytecznych informacji o kwantowych odwracalnych bramkach i układach, syntezie i optymalizacji takich układów można znaleźć w cytowanych artykułach i książkach. Algorytm Grovera ma wiele wariantów takich jak wzmocnienie amplitudy (amplitude amplification) czy inicjalizacja stanu kwantowego (quantum initialization) do stanów innych niż $|0\rangle^n$ czy $(|0\rangle + |1\rangle)^n$.

Interesująca praca[7] rozszerza idee Grovera na problemy, które mają strukturę. Różne uogólnienia są na przykład używane w kwantowych sieciach neuronowych[8] i sieciach bayesowskich[9]. Przedstawione idee projektowania wyroczni czy układów stosują się też do wielu z tych rozszerzeń.

Algorytmy kwantowe realizowane z wyroczniami są potencjalnie szybsze niż klasyczne układy boolowskie, ponieważ wykorzystują równoległość kwantową wynikającą z superpozycji. Algorytmy te operują na wszystkich wektorach przestrzeni rozwiązań równolegle (tak jakby dla każdego mintermu funkcji boolowskiej w wyroczni istniał osobny klasyczny procesor wyliczający wartość tej funkcji). Minterm to binarny wektor reprezentujący iloczyn wszystkich zmiennych tej funkcji lub negacji zmiennych. Na przykład dla funkcji 4 zmiennych jednym z 16 mintermów jest *a'bc'd* reprezentowany przez 0101.

Podczas gdy klasyczna wyrocznia potrzebowałaby N razy sprawdzać elementy przestrzeni rozwiązań o N elementach jeden po drugim, równoważna wyrocznia w algorytmie Grovera jest wywoływana tylko $\sqrt{(N)}$ razy, co oznacza kwadratowe przyspieszenie. Zatem wyrocznia kwantowa, iterowana wystarczającą liczbę razy jako część pętli Grovera, znacznie zwiększa prawdopodobieństwo znalezienia jednego z rozwiązań problemu w pojedynczym pomiarze. Pomiar ten jest dla wszystkich kubitów zmiennych wejściowych, a czasem mierzone są też dodatkowe kubity.

Dotychczas omawialiśmy wariant algorytmu Grovera z jednym rozwiązaniem. W następnym artykule z cyklu omówimy problemy z wieloma rozwiązaniami. Zauważmy, że $N \leq 2^n$, gdzie n jest liczbą kubitów potrzebnych do zakodowania rozwiązywanego problemu. Jak wspomniano, algorytm Grovera daje kwadratowe przyspieszenie w porównaniu do tego samego problemu rozwiązywanego klasycznie. Zauważmy jednak, że to kwadratowe przyspieszenie odnosi się jedynie do problemów ślepego pełnego przeszukiwania przestrzeni rozwiązań. Algorytm Grovera nie jest zatem panaceum. Kiedy chcemy zastosować ten algorytm do rozwiązania nowego problemu, musimy się najpierw zapytać o złożoność najlepszego znanego obecnie algorytmu klasycznego dla rozwiązania tego problemu.

Konkludując, algorytm Grovera jest stosowalny do większej klasy problemów niż inne algorytmy kwantowe, jest używany przez wiele innych algorytmów kwantowych. Istnieje wiele rozszerzeń i modyfikacji algorytmu Grovera. Zaznajomienie się z tym algorytmem jest idealnym początkiem uczenia się informatyki kwantowej.

7 Cerf, N.J., Grover, L.K., Williams, C.P.: Nested quantum search and NP-hard problems. *Applicable Algebra in Engineering, Communication and Computing*, 2000, 10(4/5), s. 311–338.

8 Lagaris, I.E., Likas, A., Fotiadis, D.I.: Artificial neural network methods in quantum mechanics. *Computer Physics Communications*, 1997, vol. 104, s. 1–14.
Beer, K., Bondarenko, D., Farrelly, D., Osborne, T.J., Salzmann, R., Scheiermann, D., Wolf, R.: Training deep quantum neural networks. *Nature Communications*, 2020, 11, 808.
Ezhov, A., Ventura, D.: Quantum Neural Networks. W: N. Kasabov (red.), *Future Directions for Intelligent Systems and Information Science* (s. 213–235). Haidelberg 2000, Physica-Verlag.

9 Tucci, R.: Quantum bayesian nets. *Int. J. Modern Phys,* 1995, vol. B9, s. 295–337.

Konkurs PTI na najlepsze prace magisterskie z informatyki rozstrzygnięty

Pierwszą nagrodę XXXVIII edycji Konkursu zdobył mgr Jan Kopański za pracę „Optymalizacja szeregowania zadań na superkomputerach z uwzględnieniem buforów impulsowych", wykonaną w Uniwersytecie Warszawskim.

Tematyka zwycięskiej pracy magisterskiej „Optimisation of job scheduling for supercomputers with burst buffers" dotyczy zagadnienia szeregowania zadań na superkomputerach z uwzględnieniem buforów impulsowych, które są dodatkowym poziomem pamięci pomiędzy pamięcią operacyjną a pamięcią zewnętrzną, wykorzystującym równoległe systemy plików oraz dyski twarde.

Sposób umieszczenia buforów impulsowych w architekturze superkomputera wpływa na kolizje ruchu sieciowego między węzłami obliczeniowymi i do systemu plików, co przekłada się na spowolnienie wykonania zadań (obliczeń równoległych). Przydziałem zadań do superkomputerów zajmują się systemy kolejkowe, realizujące różne algorytmy szeregowania zadań (obliczeń) równoległych. Algorytmy te powinny uwzględniać istnienie buforów impulsowych, które z jednej strony mogą istotnie przyspieszyć operacje wejścia/wyjścia, a z drugiej – źle obsługiwane mogą obniżyć efektywność obliczeń równoległych. Jest to problem szczególnie istotny w świetle zwiększającej się, w wyniku postępu technologicznego, różnicy pomiędzy wydajnościami zasobów obliczeniowych a operacji wejścia/wyjścia (co podkreślają prace naukowe ostatnich lat). Pomimo rozwoju rzeczywistych architektur superkomputerów, jak również koncepcji naukowych, stosowane systemy zarządzania zasobami i zadaniami umożliwiają jedynie marginalne wsparcie dla szeregowania zadań z buforami impulsowymi.

Autor, zmotywowany obserwacją, że powszechnie stosowana procedura szeregowania z dopełnianiem (backfilling) pomija rezerwacje buforów impulsowych w istniejących systemach szeregowania zadań, postanowił zająć się tym tematem.

Najważniejszym, oryginalnym osiągnięciem autora, opisanym w pracy, jest opracowanie i przetestowanie algorytmu szeregowania zadań na superkomputerach, uwzględniającego bufory impulsowe, wykorzystującego optymalizację metodą symulowanego wyżarzania. Wyniki ewaluacji pokazały, iż wybrane metryki, takie jak średni czas oczekiwania czy spowolnienie, zostały poprawione o ponad 20% w porównaniu do standardowych podejść, co należy uznać za istotny wynik.

dr inż. Zbigniew Szpunar
sekretarz Komisji Konkursowej

– Autor wykazał się dużą wiedzą o architekturze superkomputerów, o interakcjach między ruchem sieciowym w superkomputerze a czasem wykonania zadań równoległych, o systemach kolejkowych i wykorzystywanych w nich algorytmach szeregowania. Wykazał biegłość w wykorzystaniu narzędzi symulacyjnych i analizy danych. Praca jest na wysokim światowym poziomie badawczym, co potwierdza jej opublikowanie w ramach konferencji Euro-Par 2021 – czytamy w jednej z recenzji pracy.

Jury konkursu uznało, że praca pokazuje znakomite przygotowanie autora do prowadzenia badań w dziedzinie systemów komputerowych i stanowi bardzo dobry przykład połączenia problemów teoretycznych i praktycznych na wysokim poziomie.

Wszystkim laureatom Konkursu serdecznie gratulujemy!

POLSKIE TOWARZYSTWO INFORMATYCZNE

Wyniki XXXVIII Ogólnopolskiego Konkursu Polskiego Towarzystwa Informatycznego na najlepsze prace magisterskie z informatyki.

Do konkursu przyjęto 25 prac wykonanych w roku akademickim 2020/2021
w dziewięciu krajowych wyższych uczelniach.
Komisja Konkursowa w składzie:
prof. ucz. dr hab. Zygmunt Mazur (przewodniczący), dr inż. Marek Bolanowski,
prof. dr hab. inż. Maciej Drozdowski, prof. dr hab. inż. Zbigniew Huzar, prof. dr hab. inż. Andrzej Kwiecień,
prof. ucz. dr hab. inż. Lech Madeyski, dr hab. Marcin Paprzycki, prof. ucz. dr hab. Jakub Swacha,
dr inż. Zbigniew Szpunar (sekretarz) oraz dr hab. inż. Bartosz Walter,
uwzględniając opinie recenzentów prac konkursowych, ustaliła laureatów konkursu.

Pierwszą nagrodę w wysokości 5000 zł otrzymał
mgr Jan Kopański
za pracę **„Optimisation of job scheduling for supercomputers with burst buffers"**
wykonaną w Uniwersytecie Warszawskim
(Wydział Matematyki, Informatyki i Mechaniki,
Instytut Informatyki;
promotor: dr hab. Krzysztof Rządca).

Drugą nagrodę w wysokości 4000 zł otrzymał
mgr inż. Andrzej Szaflarski
za pracę **„ Algorytmy detekcji zespołu QRS w sygnale elektrokardiogramu"**
wykonaną w Akademii Górniczo-Hutniczej
im. Stanisława Staszica w Krakowie
(Wydział Informatyki, Elektroniki i Telekomunikacji,
Instytut Informatyki;
promotor: prof. ucz. dr hab. inż. Marek Miśkowicz).

Trzecią nagrodę w wysokości 3500 zł otrzymał
mgr inż. Bartosz Kusek
za pracę **„Algorithms for Approval-Based Elections with Structured Preferences"**
wykonaną w Akademii Górniczo-Hutniczej
im. Stanisława Staszica w Krakowie
(Wydział Informatyki, Elektroniki i Telekomunikacji,
Instytut Informatyki;
promotor: prof. dr hab. inż. Piotr Faliszewski).

Trzy równorzędne wyróżnienia po 2500 zł otrzymali:
mgr inż. Bartosz Drzazga
za pracę **„Isogeny-based cryptography – chosen schemes"**
wykonaną w Politechnice Wrocławskiej
(Wydział Podstawowych Problemów Techniki,
Katedra Podstaw Informatyki;
promotor: dr hab. inż. Łukasz Krzywiecki);

mgr Daniel Gutowski, mgr Artur Jamro i mgr Wojciech Kordalski
za pracę **„Toward Cycle-Accurate Emulation of the ARM Cortex-M3 Processor Instructions and Memory"**
wykonaną w Uniwersytecie Warszawskim
(Wydział Matematyki, Informatyki i Mechaniki,
Instytut Informatyki;
promotor: dr hab. Konrad Iwanicki);

mgr inż. Hubert Krzyżanowski i mgr inż. Łukasz Pięta
za pracę **„Odkrywanie charakterystyk User-Defined Functions"**
wykonaną w Politechnice Poznańskiej
(Wydział Informatyki i Telekomunikacji,
Instytut Informatyki;
promotor: prof. ucz. dr hab. Robert Wrembel).

Fundatorem nagród jest Polskie Towarzystwo Informatyczne.

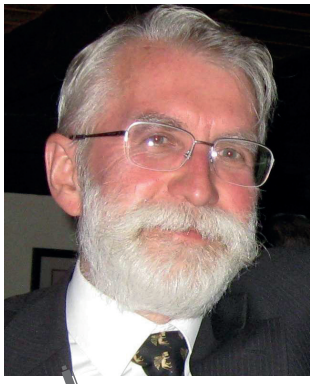
O dostawcach wysokiego ryzyka

25 stycznia br. na spotkaniu Klubu Informatyka Oddziału Mazowieckiego PTI odbyła się dyskusja na temat ekspertyzy „Zagrożenia dla cyberbezpieczeństwa sieci telekomunikacyjnych w Polsce ze strony potencjalnych dostawców wysokiego ryzyka", którą w ramach Izby Rzeczoznawców przygotowali Jarosław Mojsiejuk i Wiesław Paluszyński. Ekspertyzę przeczytałem, w dyskusji zabierałem głos, chcę także podzielić się swoimi wątpliwościami w „Domenie".

Mówiąc po polsku i nieco upraszczając – chodzi o to, która firma będzie dostawcą sprzętu i oprogramowania dla polskich sieci 5G. A dokładniej – która zostanie dopuszczona do udziału w przetargach.

Deklaracja bezstronności

Na wstępie informuję, że nie łączą mnie żadne związki ani z Huawei, ani z Ericssonem, czyli dwoma głównymi liczącymi się dostawcami (z pozostałymi też nie). Dzisiejszą Szwecję lubię i szanuję (choć nigdy tam nie byłem, a Szwedzi nam niegdyś złupili Warszawę). Dzisiejszych Chin nie znoszę, tak jak innych krajów totalitarnych. Nie wybieram się tam w celach turystycznych, choć to teraz modne, bo wizja podróżowania po obozie koncentracyjnym (nawet o złagodzonym reżimie) zupełnie mnie nie pociąga. Zdaję sobie także sprawę, że gospodarka chińska ma mało wspólnego z wolnym rynkiem i mam cichą nadzieję, że po wyczerpaniu prostych rezerw okaże się nieefektywna, tak



Jarosław Deminet

informatyk od 1979 r., bywał nauczycielem akademickim, urzędnikiem, szefem działów produkujących oprogramowanie w korporacji, konsultantem biznesowym, publicystą. Członek założyciel PTI, obecnie pracownik Rządowego Centrum Legislacji i sekretarz Zarządu Oddziału Mazowieckiego PTI, rzeczoznawca PTI nr 13.

jak w każdym innym kraju totalitarnym, bez demokratycznych władz, prywatnych niezależnych banków i niezawisłych sędziów gwarantujących firmom równość szans.

To napisawszy, muszę jednak stwierdzić, że gospodarka ta i jej produkty są bardzo istotnym elementem światowego rozwoju. Nie chodzi tylko o bawełniane koszulki czy komputery Lenovo. Przypominam, że w Polsce wejście chińskich firm na rynek budowlany pozwoliło rozbić oligopol kilku konsorcjów (udowodnione zmowy cenowe kamuflowane podawanymi numerami pokojów). Chińczycy ostatecznie źle na tym wyszli, bo lokalni dostawcy i podwykonawcy w obronie dotychczasowego układu zgodnie ich zbojkotowali. To oczywiście dramatycznie utrudniło prace i podniosło koszty, Chińczycy ponieśli straty i wycofali się, ale stary układ (chyba) już nie wrócił i ceny budowy autostrad jakoś się ustabilizowały.

Napiętnowany Huawei

Tak się składa, że firma Huawei jest jednym z dwóch głównych dostawców systemów dla sieci komórkowych 5G, często wybieranym przez operatorów, szczególnie ze względów cenowych. Jako firma chińska jest podejrzewana i oskarżana o zachowania dywersyjne, które mogą zagrażać bezpieczeństwu użytkowników czy wręcz całych krajów. Amerykanie wpisali ją na czarną listę, Google cofnął licencję na Androida i zablokował dostęp do sklepu Google Play, co oczywiście dramatycznie zmniejszyło atrakcyjność jej telefonów komórkowych. W Kanadzie na żądanie USA zatrzymano na 3 lata córkę założyciela koncernu pod zarzutem nielegalnej (w USA) współpracy z Iranem, ale w końcu pozwolono jej wyjechać. Były dyrektor firmy w Polsce kilka lat temu został oskarżony o szpiegostwo, aresztowany, zwolniony i znów aresztowany. Proces się ciągnie niespiesznie i przy drzwiach zamkniętych, ostatnie doniesienia prasowe są chyba sprzed półtora roku. Niestety, Amerykanie mają – oględnie pisząc – dość specyficzny stosunek do zasad wolności i równości w handlu międzynarodowym, więc na ich zarzuty należy patrzeć ostrożnie.

> *Bez wątpienia największą wartość merytoryczną ma opis kontekstu technicznego bezpieczeństwa sieci telekomunikacyjnych.*

Żeby było jasne: nie mam żadnej wątpliwości, że Huawei nie może działać bez życzliwości chińskich władz komunistycznych, a ta życzliwość może mieć swoją cenę. Wśród personelu bez wątpienia są agenci wszelkich możliwych chińskich tajnych służb. Można się obawiać, czy w urządzeniach Huawei nie zamontowano jakichś systemów szpiegujących, analizujących pakiety danych i przesyłających je do Pekinu – albo blokujących system w odpowiedzi na zdalne polecenie. Możliwość audytu tak skomplikowanych urządzeń może budzić wątpliwości. Takie samo podejrzenie można jednak mieć co do komputerów Lenovo czy samochodów Volvo (to już od dawna chińska firma). Mam nadzieję (choć nie pewność), że w przypadku firm z wolnego świata sytuacja wygląda lepiej, bo prezesom w USA czy Szwecji łatwiej (co nie znaczy, że łatwo) odrzucić takie propozycje ze strony swych rządów, no a poza tym z dwojga złego wolę być podglądany przez Amerykanów czy Szwedów niż przez komunistycznych Chińczyków.

Tak, ale…

W związku z tym powstaje pytanie: czy można i należy wykluczyć Huawei z udziału w rozbudowie akurat sieci komórkowych najnowszej generacji, co znacząco osłabi konkurencję i podniesie koszty? Nie chodzi tu o firmy państwowe – czy można zabronić prywatnym operatorom kupowania i instalowania takich systemów, nawet jeśli dotychczas korzystali z usług tego dostawcy? A w perspektywie kilku lat zmusić do zastąpienia już zainstalowanych systemów nowymi, pochodzącymi od innych, akceptowalnych firm? Czy nie jest to zmiana zasad w czasie gry (Polkomtel, dziś w grupie Cyfrowy Polsat, z urządzeń Huawei nie korzysta, więc nałożenie takiego obowiązku na pozostałych daje mu znaczne oszczędności, naruszając zasadę wolnej i uczciwej konkurencji)? Jak to zrobić zgodnie z prawem, albo jak zmienić prawo, żeby było to możliwe? To nie są proste pytania i nie ma na nie prostej, oczywistej odpowiedzi. W takiej sytuacji obaw o lobbing może być wiele, należy więc zachować szczególną ostrożność i przejrzystość postępowania. Sporo lat temu sam byłem w podobnej sytuacji: państwowy zamawiający już po rozstrzygnięciu przetargu zażądał (nieoficjalnie) zmiany jednego z poddostawców, powołując się na nieujawnione względy bezpieczeństwa. Chcę wierzyć, że tamto uzasadnienie było prawdziwe, ale nie wyglądało to elegancko.

Wątpliwości trwają, decyzji nie ma, wiewiórki donoszą, że z tego powodu ciągle nie ma przetargu na pasma dla 5G. Ma być ustawowo wprowadzone pojęcie „dostawcy wysokiego ryzyka". Taka kwalifikacja przez rządowe kolegium ds. cyberbezpieczeństwa oznaczałaby praktycznie wykluczenie firmy z rynku. Sama decyzja byłaby podejmowana bez udziału zainteresowanych firm i bez żadnej kontroli społecznej, na podstawie informacji od wiadomych służb (zapewne niejawnej), czyli w praktyce zupełnie arbitralnie. Eksperci są podzieleni, część z nich twierdzi, że lepszym rozwiązaniem jest wprowadzenie wymogów certyfikacyjnych (urządzenie psujące się może być dla bezpieczeństwa państwa równie groźne, co urządzenie szpiegujące).

Przedstawiciele firm i izb gospodarczych prowadzą intensywny wielokierunkowy lobbing, zgodnie z własnym uzasadnionym interesem.

Noblesse oblige

W takich okolicznościach powstała ekspertyza, o której pisałem na wstępie, przygotowana na zlecenie Akademii Sztuki Wojennej. Bardzo się cieszę, że to Izba Rzeczoznawców PTI, niezwiązana instytucjonalnie z żadnymi firmami, została do tego zaproszona. Pewne elementy formy i treści ekspertyzy budzą jednak moje wątpliwości.

Przede wszystkim uważam, że w przypadku takich ekspertyz autorzy powinni zachować powściągliwość w opowiadaniu się po stronie jednego rozwiązania, zwłaszcza gdy wiadomo, że sprawa jest kontrowersyjna i niejednoznaczna. Parę miesięcy temu spotkanie Klubu Informatyka było poświęcone budowie sieci 5G, a przedstawiciel Huawei spokojnie i racjonalnie przedstawiał swoje argumenty. Oczywiście konkluzja ekspertyzy może wyraźnie wskazywać, że jakieś rozwiązanie jest lepsze od innych, albo wręcz jest jedynym akceptowalnym, ale wcześniej wskazana jest bezstronność. W trakcie lektury odnoszę nieodparte wrażenie, że autorzy zbyt mocno od samego początku opowiadają się po stronie zwolenników wprowadzenia pojęcia „dostawcy wysokiego ryzyka". Może to niestety być przywołane przez przeciwników do podważenia obiektywizmu ekspertyzy i osłabienia jej wiarygodności.

PTI powinno trzymać się z dala od kwestii politycznych i koncentrować na sprawach technicznych. Przy całym moim szacunku dla autorów i ich wiedzy, razi mnie pierwsza część raportu, poświęcona geopolityce. Opis relacji Chiny – NATO czy związków firm chińskich ze służbami specjalnymi są oczywiście dla sprawy istotne, ale nie powinna ich firmować Izba Rzeczoznawców PTI, bo nie mają związku z naszymi kompetencjami (poza krótką informacją o chińskiej złośliwej aktywności cybernetycznej). Nawet wątek dotyczący polityki protekcjonistycznej tylko marginalnie dotyka przemysłu elektronicznego, a problem naruszania własności intelektualnej odnosi się do wszystkiego, nie ma związku z bezpieczeństwem i mógłby równie dobrze być podstawą do zakazania importu laptopów Lenovo (a może i bawełnianych koszulek; kto wie, czy przy produkcji barwnika nie naruszono jakiegoś europejskiego patentu). To samo dotyczy obaw o ewentualną monopolizację rynku – może ona dotyczyć równie dobrze każdego innego dostawcy.

Autorzy wskazali na potencjalne punkty ataku i przytoczyli negatywne przykłady z przeszłości Huawei i innych chińskich firm, zabrakło mi jednak danych wskazujących, czy podobnych zastrzeżeń nie zgłaszano też do innych dostawców (wspomniano Pegasusa, ale to już inna historia). Niestety, przedstawienie zgłaszanych zagrożeń z góry jako „mitów" nie brzmi dobrze w profesjonalnej ekspertyzie.

Autorzy kwestionują skutek finansowy, powołując się na raport firmy Play, przewidującej konieczność wydania raptem 900 mln zł w razie konieczności zastąpienia produktów Huawei innymi, i bagatelizują tę kwotę. Akurat ja mam telefon w Playu i nie mam złudzeń, że ostatecznie to ja poniosę te koszty, więc ta kwota na mnie działa. Wyższe wyceny, dokonane przez firmy doradcze, autorzy chyba zbyt lekko dezawuują.

Podane tu przykłady nie podważają wartości merytorycznej argumentów technicznych, opisanych bardzo szczegółowo. Wiarygodność Huawei może budzić wątpliwości. Być może wprowadzenie praktycznego zakazu korzystania z usług pewnych firm jest niezbędne. Ja po przeczytaniu ekspertyzy nie potrafiłbym zająć jednoznacznego stanowiska za lub przeciw, choć rozumiem i doceniam zagrożenia. Chętnie przeczytałbym stanowisko firmy Huawei w tej sprawie.

Na marginesie – jako informatyk niedowierzający innym informatykom nie jestem pewien, czy nie należy bardziej się obawiać indywidualnych programistów (lub ich zespołów), np. zatrudnionych w europejskich czy amerykańskich firmach. Mogą oni w praktyce bezkarnie pozostawiać w swoim kodzie zakamuflowane luki czy otwarte drzwi kuchenne, których zidentyfikowanie wcale nie będzie łatwe. I czynią to bez ryzyka. Firma, która świadomie decyduje się na takie samo postępowanie, ryzykuje bardzo dużo – w przypadku wykrycia jej renoma dramatycznie spadnie.

Ekspertyza PTI zapewne będzie bardzo starannie analizowana i – mam nadzieję – pomoże politykom i urzędnikom podjąć najlepszą decyzję. Będzie oceniana także przez przeciwników proponowanego rozwiązania i nie chciałbym, żeby ktokolwiek mógł zakwestionować jej obiektywizm. Wolałbym, aby w przyszłości zachowywać większą ostrożność i powściągliwość.

Ekspertyza jest dostępna pod adresem:

https://portal.pti.org.pl/dostawcy-wysokiego-ryzyka/

Wiesław Paluszyński
prezes PTI

Fot. Beata Sołtys

„Gry" wojenne

Jako mały chłopiec w latach 50. słuchałem przestraszonych głosów moich rodziców (ojciec – lwowiak i powstaniec warszawski, mama – harcerka z Zagłębia Dąbrowskiego): czy będzie wojna, czy wejdą, czy trzeba będzie uciekać, ale gdzie? Atmosfera tego strachu powraca, gdy widzę uchodźców z Ukrainy. Zapewne nie tylko ja doświadczam déjà vu – odczucia, że przeżyłem to już wcześniej, połączonego z pewnością, że to niemożliwe.

Przyzwyczailiśmy się do wirtualnych wojen, które umożliwił rozwój informatyki. Wcześniejszym próbom, realizowanym początkowo w kinematografii, daleko było do realizmu. Dzisiaj możemy mieć w kinie, telewizorze czy komputerze pełnowymiarową wojnę. Zarówno tę fikcyjną, ale pokazaną realistycznie, jak w „Gwiezdnych wojnach", „Diunie" czy w ekranizacji prozy Tolkiena, jak i tę prawdziwą, odtworzoną w komputerowej animacji, jak np. ostatnio w filmie „Dunkierka". Oglądamy wojnę w telewizji, nadal przecież emitowane są seriale „Czterej pancerni" czy „Stawka większa niż życie".

W świecie gier komputerowych walczymy – nasze dzieci i wnuki – realistycznymi czołgami, latamy samolotami F16, bombardujemy i niszczymy wroga. Ofiary tej wirtualnej wojny są mało widoczne, widoczne są sukcesy. Na tych wojnach w komputerach czy na konsolach informatycy nieźle zarabiają. Wydawało się nam, że wojna już taką pozostanie, a uczestniczący w niej młodzi ludzie będą dostawali kolejne „życia", aby móc odnosić wojenne sukcesy.

I raptem na ekranach naszych telewizorów, tabletów i telefonów pojawiła się prawdziwa wojna. Wojna rozpoczęta przez zakłamanego agresora, wykorzystującego w swojej narracji kłamstwo, ale też wysokie technologie, wspierane systemami informatycznymi, pochodzącymi również z krajów demokratycznych. Mordującego cywilów, kobiety i dzieci rakietami wykorzystującymi komponenty stworzone przez informatyków.

Ofiary tej wojny w realu nie mają kolejnych „żyć". Widzimy gigantyczne zniszczenia, uciekających ludzi, mordowanych cywilów. Widzimy, bo rozwój informatyki na to pozwala, widzimy, bo działają – pomimo starań agresora – sieci komórkowe, słyszymy, bo rozmowy żołnierzy agresora są podsłuchiwane, a drony, które służyły do zabawy, dokumentują zbrodnie wojenne. Grupa anonimowych informatyków prowadzi prywatną wojnę z agresorem, atakując wraże systemy informatyczne, zdobywając i publikując dowody jego kłamstw i manipulacji. Agresor blokuje te kanały komunikacji, bo buduje przychylność dla swoich działań na fałszywym obrazie rzekomych sukcesów. Tę wojnę toczą nie tylko państwa i ich wojska, toczą ją zwykli ludzie, którzy uznali, że walka z imperialnym, XIX-wiecznym pojmowaniem świata jest też ich walką.

Miliony kobiet i dzieci szukających domu w Polsce to sceny, których nie było w grach. To rzeczywistość, w której – obok gigantycznego wysiłku zwykłych ludzi – informatyka staje się niezbędnym narzędziem, zarówno ta rządowa, pomagająca ogarnąć system udzielania pomocy, jak i ta społeczna, pomagająca znaleźć informację, pokierować do nowych miejsc zamieszkania, zarządzić przesyłaną pomocą. My – informatycy – pomagamy, jak potrafimy i możemy, piszemy niezbędne programy po 24 godziny na dobę, zdobywamy komputery dla ukraińskich dzieci zaczynających naukę w naszych szkołach. Pomagamy w ramach wolontariatów, zbieramy i przesyłamy niezbędny do walki i obrony sprzęt informatyczny, telefony, komputery.

Gdy jednak mamy wolną chwilę, zastanawiamy się, czy nie przyczyniliśmy się przypadkiem do tego koszmaru, który widzimy? Jak dalej pracować, aby efekty zastosowania kluczowych technologii, np. sztucznej inteligencji, nie przyczyniały się do ludzkich nieszczęść, do budowania kolejnych wersji zabójczych systemów? Czy da się budować tylko systemy obronne? Niedawno widzieliśmy, jak informatyka pomogła przeciwdziałać epidemii i umożliwiła pracę w trudnym epidemicznym czasie. Dzisiaj obserwujemy wojnę hybrydową z wykorzystaniem tych samych mediów, które niedawno służyły nam w przezwyciężaniu katastrofy. Nieuchronnie zbliża się czas odpowiedzi na pytania związane z etyką naszego zawodu…

Język oryginalny

Z tytułowym pojęciem, przez pewien czas wywołującym mój niepokój, zetknąłem się nie tak dawno temu. Dotyczyło to spraw wikimedijnych i dokumentu *Universal Conduct of Code* oraz jego tłumaczeń. Padło wtedy na forum polskiej wikipedii stwierdzenie, że ów *Universal Conduct of Code* jest napisany w języku oryginalnym, czyli angielskim. Stąd można było, oczywiście nadmiarowo, wnioskować, że jest to język prawdziwy, nieomalże jak w „Ziemiomorzu" Ursuli Le Guin.

Janusz Dorożyński

adiunkt badawczo-dydaktyczny Instytutu Informatyki Uniwersytetu Kazimierza Wielkiego w Bydgoszczy. Absolwent Moskiewskiego Instytutu Subtelnej Technologii Chemicznej im. Łomonosowa (obecnie część Moskiewskiego Uniwersytetu Technologicznego). W 1984 r. na tej uczelni uzyskał stopień doktora nauk technicznych. W pracy zawodowej do 2017 r. związany z przemysłem informatycznym. Członek PTI od 1985 r.

Więc konsekwentnie nasz język ojczysty (a jeśli ktoś woli – matczyny lub rodzimy) jest językiem nieoryginalnym, czyli nieprawdziwym. Mogłoby to wywołać dyskomfort poznawczy zdecydowanie mniej przyjemny niż ten, który był udziałem *monsieur* Jourdaina.

Rzeczony niepokój powstał zapewne dlatego, że nie jestem biblistą. Dla biblisty w sposób oczywisty mowa polska w kontekście Biblii jest językiem nieoryginalnym. Oczywiście niepokój ów ulotnił się dość szybko, jak tylko świadomie zarejestrowałem, iż właśnie kontekst jest tu istotny, a nie choćby oczywisty synonim przymiotnika „oryginalny".

Jak by jednak nie było, to język angielski, nazwijmy go mniej kontrowersyjnie światowym, jest zwłaszcza w informatyce oraz publikacjach naukowych współczesnym nomen omen *lingua franca*, czyli właśnie międzynarodowym. Z wszystkimi tego konsekwencjami. Również skutkiem takim, który nosi miano kolonizacji językowej. Historycznie kolonizowanie, a więc zawładnięcie i przeobrażanie pewnej społeczności przez inną, było związane z przemocą, oznaczało stosowanie przymusu, było widoczne i zazwyczaj rodziło mniejszy lub większy, ukryty czy gwałtowny opór. W całym spektrum kolonizowania zazwyczaj występowało, również wymuszane, przenikanie obcego języka do języka zawłaszczonej społeczności jako działanie pochodne, wtórne. Bliskim nam przykładem historycznym jest proces stopniowego rugowania języka polskiego z procesu kształcenia na terenie zaboru rosyjskiego, czyli początkowo Królestwa Polskiego, a w końcu Kraju Nadwiślańskiego. Ze względu na pewną początkową autonomię Kongresówki szkolnictwo funkcjonowało w języku polskim i oczywiście z lekcjami języka polskiego, aby ostatecznie funkcjonować już tylko w języku rosyjskim, choć z zachowanym nauczaniem języka polskiego w języku rosyjskim (sic!). Nie wiem, czy w owym czasie publikowano prace naukowe z polonistyki (o ile wówczas oficjalne istniała) w języku rosyjskim, ale chichot historii jest przedni. Niedawno poszukiwałem materiałów na temat pewnego problemu języka polskiego, czyli z zakresu polonistyki, i dość szybko udało mi się odszukać odpowiednie artykuły naukowe. Nie bez zdziwienia – wszystkie w języku angielskim. Tak, wiem, punkty, punkty, punkty, ale czyż nie mamy tu przejawu kolonizacji języka polskiego jako zjawiska obecnie niepochodnego, ale samodzielnego, samorzutnego i dobrowolnego?

Podobnie można postrzegać tę kwestię w polskiej informatyce. Ale tylko podobnie, gdyż w odniesieniu do mowy polskiej, będącej przedmiotem zainteresowania polonistyki, ogólnie nie występuje zjawisko tworzenia pojęcia w języku oryginalnym. W informatyce tak właśnie jest. Terminy powstają, ustawicznie, w języku angielskim,

a następnie dość szybko kolonizują, oczywiście nie tylko polski, lecz także inne języki. Początkowo przebiega to zazwyczaj poprzez zapożyczenie wprost, łącznie z oryginalną pisownią, co w mowie odzwierciedlane jest mniej lub bardziej fonetyczne. A następnie bywa już różnie – pozostaje jak było albo termin otrzymuje pisownię fonetyczną, albo bywa jednak przetłumaczony. Tylko w tym ostatnim przypadku nie występuje kolonizacja językowa.

> *Prowadzi to do funkcjonowania w naszym informatycznym środowisku zawodowym – moim zdaniem w dużej części bezrefleksyjnie – specyficznego socjolektu, czyli wolapiku, a mówiąc bez ogródek – żargonu.*

Niezależnie od oceny tego zjawiska, żargon ów ułatwia komunikację we własnym kręgu, niekiedy poprzez zamianę dłuższych wyjaśnień na jedno czy dwa słowa. Jednocześnie taka hermetyzacja języka mówionego może dawać niektórym osobom z naszego kręgu poczucie wyższości z powodu władania mową tajemną, a stąd już tylko krok do przekonania, że jest to także dowód na posiadanie wiedzy tajemnej.

O ile to, że informatycy posiadają wiedzę nietajemną, ale specjalistyczną, nie budzi kontrowersji, to potencjalne poczucie przewagi czy lekceważenia wobec osób ze świata dla informatyki zewnętrznego jest, mówiąc delikatnie, po prostu żenujące. Zwłaszcza jeśli pamiętamy słowa prof. Władysława Turskiego, że informatyka i informatycy odgrywają rolę służebną wobec użytkowników. A trudno tę funkcję spełniać, gdy taki służebnik używa w komunikacji z użytkownikami języka niezrozumiałego, niczym ślusarz ze znanego felietonu Juliana Tuwima.

Sam byłem świadkiem egzemplifikacji tego zjawiska, gdy pewna hurtownia z południa Polski rozważała zwrot zakupionego przeze mnie w jednej z warszawskich firm oprogramowania Novell Netware Lite. Negocjować te sprawę pojechał prezes hurtowni, skądinąd obrotny i skuteczny handlowiec. Wrócił jak zbita psina i podsumował: – *Człowiek, z którym rozmawiałem, chyba mówił po polsku, ale nie zrozumiałem ani jednego słowa.*

Niestety, wspomniane wyraziste przejawy kolonizacji polskiego języka informatycznego nie oddają całej perspektywy. Składa się na nią nawet nie oczekiwanie (niektórych) polskich informatyków-teoretyków, ale wręcz pewność, że posługują się nie naszym informatycznym wolapikiem, ale językiem światowym i jego informatyczną terminologią. Jakiś czas temu podczas jednej z zasłużonych konferencji PTI – KKIO moją uwagę zwrócił ciekawy referat o przetwarzaniu reguł biznesowych w naturalnym języku regułowym w rodzaju SBVR SE w modele biznesowe. Wprawdzie i zgłoszony artykuł, i wygłoszone omówienie było w języku światowym (bo punkty!), ale gdy w dyskusji zapytałem, czy określenie „język naturalny" dotyczy również naszego tubylczego (konferencja była w Białymstoku), to tak à propos języka, to usłyszałem, że oczywiście nie, gdyż liczy się tylko język światowy i nikt (informatycznie-naukowo) innym nie będzie się zajmował.

Relacjonowanie stanu rzeczy bywa zajmujące, budzi różne emocje, można też na tym poprzestać. Ale może też być inspiracją do działania. Nawet jeśli poniewczasie – nigdy nie jest za późno. Zwłaszcza mając w pamięci, jak polskie rodzące się środowisko informatyczne usilnie, acz skutecznie, dążyło do tłumaczenia terminologii angielskiej. Jak Stefan Paszkowski przy okazji polskiej publikacji specyfikacji języka Algol 60 skrupulatnie, na karteczkach, analogowo, uzgadniał – wypytując wszystkich zainteresowanych – najodpowiedniejsze polskie terminy. Taką troskę wykazywali (i wykazują nadal) inni polscy informatycy z naszego, aczkolwiek powstałego później niż czasy Algolu 60, towarzystwa. To przecież choćby i prof. Wojciech Cellary, i dr inż. Wacław Iszkowski, i prof. Andrzej Jacek Blikle, i Andrzej Dyżewski przewodniczący Sekcji Terminologicznej PTI. Tym niemniej odczuwam spory niedosyt. Również wobec siebie, członka PTI, zwłaszcza że sprawy polskiej terminologii informatycznej były mi zawsze bliskie, jeszcze w czasach Komisji Terminologicznej PTI prof. Antoniego Mazurkiewicza, która niestety ostatecznie nie podjęła – poza pierwszym spotkaniem w PKiN – działalności.

Pomimo tego niedosytu uważam, że jako PTI możemy i powinniśmy teraz skutecznie podejść do stworzenia dostępnego, otwartego, normatywnego, gdyż firmowanego przez towarzystwo naukowe, polskiego zasobu terminologii informatycznej, a może nawet glosariusza. Byłoby to wsparcie i dla nas informatyków, i dla użytkowników. I dla polskiej wikipedii, która notabene może być też postrzegana jako utworzony ad hoc zasób terminologiczny, po części jednak z terminami oryginalnymi, z hasłami należącymi do gniazda (drzewa) kategorii „Informatyka". Wykaz podkategorii tego gniazda to trochę ponad 1600 pozycji. Ale to już jest kolejny temat.

Tym niemniej …

Potrzeba stworzenia polskiego zasobu terminologicznego nie neguje pozycji języka światowego, choć co i rusz pojawiają się zapowiedzi jego Środkowej detronizacji. Publikowanie w tym języku, zwłaszcza prac naukowych, a informatycznych w szczególności, jest oczywistością. Tyle że publikować w języku angielskim należy również – bo to też tworzy terminologię – a nie wyłącznie, jak nawołuje z głębokim zaangażowaniem prof. Marcin Paprzycki, jeden z twórców sukcesu anglojęzycznej konferencji FedCSIS (za 70 punktów).

Michał Ogórek
satyryk i felietonista, od 1989 r. związany z „Gazetą Wyborczą". Obecnie pisuje w „Angorze". Autor wielu książek. Ostatnio wydał „Sto lat! Jak czciliśmy przywódców w ostatnim stuleciu", o kulcie przywódców – od Piłsudskiego przez Bieruta i Gomułkę po braci Kaczyńskich.

Więcej poufałości niż znajomości

Komputer jest nam rzeczą najbliższą od kołyski. Pamiętam, że kiedy mojemu małemu synkowi czytałem wiersz Brzechwy „pewna żaba była słaba", to zalecenie „niech pani nie siada przy pompie" rozumiał jako „przy kompie", bo słowa pompa nie znał.

Komputer znaczy dziś tak dużo, że właściwie nie wiadomo co. Nikt nie widzi już komputera w swoim samochodzie, mierniku kroków na przegubie itd. Ani w telefonie. Ale właśnie: czy telefonie? Czym jest to coś, w co wpatrujemy się jak sroka w gnat i z czego nie spuszczamy wzroku? Nazywanie tego telefonem to jak spostrzeganie w kompie – pompy: przecież to nie tyle znacznie więcej, co właściwie już w ogóle nie to. Ja mam przestarzałego ajfona, ale mimo że taki stary, nigdy nie powiedziałem ani nie pomyślałem o nim jako o ajfonie, choć w Ameryce mówią tak powszechnie. U nas przyjął się smartfon, ale nie oddaje to natury tego urządzenia, które – na tym jednym swoim ekranie – ma tak wiele twarzy. Co ja więc noszę w kieszeni – nie wiem. Gdybym ja chociaż wiedział o nim kilka procent tego, co ono o mnie!

Z ulicznych obserwacji i badań sondażowych wynika, że to już odrębna dziedzina życia, całkiem różna np. od korzystania z „pełnoprawnego" komputera. Telefon to uproszczona i maksymalnie ułatwiona wersja komputera, taka trochę zabawkowa. Badania pokazały, że młodzi ludzie z „prawdziwego" komputera statystycznie korzystają kilka razy w miesiącu, co przy stałym, tak na oko osiemnastogodzinnym na dobę ślepieniu w jego wersję kieszonkową oznacza, że jest on dla młodzieży czymś tak rzadkim, jak dla nas w latach 90. ubiegłego wieku. Wyniki te w czasach nauki zdalnej wydają się aż niemożliwe, ale takie właśnie podał zespół prof. Jacka Pyżalskiego z UAM w Poznaniu (cytuję za „Tygodnikiem Powszechnym" z 20 lutego br.).

Z telefonu się korzysta, a na komputerze się pracuje. Jest to taka różnica, jak między kupieniem chińskiej zupki a przyrządzeniem obiadu. Niezwykle interesujące badania prof. Pyżalskiego dowodzą – wbrew potocznym przekonaniom – bardzo niskich kompetencji cyfrowych młodego pokolenia. Może to nawet (dość małostkowo) uleczyć trochę kompleksy takich dziadersów, jak ja, którzy dawno uznali, że z młodymi nie mają w sieci żadnych szans. Okazuje się bowiem, że nastolatki są bardzo specyficznymi użytkownikami – czy raczej nawet klientami – całej cyfrowej sfery. Nic a nic nie dziwi mnie to, że tylko jedna czwarta nastolatków – i to rzadko – odwiedza strony informacyjne, bo sam nieskutecznie szukam raczej sposobu, jak **nie** dowiadywać się z telefonu różnych rzeczy, z którymi on mnie obowiązkowo zapoznaje. Być może to jest ta ich kompetencja cyfrowa, aby umieć podczas dni i nocy spędzanych na dłubaniu palcem w obrazkach nawet przypadkiem nie trafić nigdy na nic poważnego.

Jakoś tam mimochodem i w ukryciu spełnia się ta dosyć ponura prognoza rozwojowa dla świata, że rozpadnie się on na ekskluzywną, miniaturową część ludzi twórczych, którzy zaprogramują całą rzeszę pozostałych, jacy oddadzą się w ich władanie, nawet o tym nie wiedząc. Co więcej: mając przeświadczenie o swojej nowoczesności, podmiotowości i nadążaniu za trendami… Rysuje się na horyzoncie taki podział społeczny, jak w feudalizmie, czy może nawet w niewolnictwie, kiedy wydostanie się z jednej niszy do innej było prawie niemożliwe i ludzie już rodzili się skazani na dalszy swój los. Na takich, którzy będą to wszystko kontrolować i takich, którzy nie będą mieli prawa nic z tego rozumieć. Jest też oczywiście możliwy jeszcze gorszy scenariusz, że również plemieniu informatyków, jak uczniom czarnoksiężnika, wymknie się to wszystko spod kontroli i już nikt nie będzie nad tym panował. Mniejsza jest groźba, że nie-informatycy obalą znienawidzonych nowych panów, bo musieliby to robić w sieci, czego nie będą mogli umieć, i nowe powstanie Spartakusa jako powstanie Spectrusa nawet się nie zacznie.

Całe to zamieszanie terminologiczne z „pokoleniem cyfrowym", myleniem tropów i mieszanie komputera z telefonem tylko temu sprzyja. Dzięki temu wydaje nam się, że z komputerem jesteśmy za pan brat, podczas gdy on traktuje nas jak kogoś do obsługi.

PREZESI ZAPRASZAJĄ...

CYKL WEBINARÓW
O INFORMATYCE, CYBERBEZPIECZEŃSTWIE ORAZ PRAWIE NOWYCH TECHNOLOGII

PRZYGOTOWANY PRZEZ
POLSKIE TOWARZYSTWO INFORMATYCZNE,
ZWIĄZEK CYFROWA POLSKA,
AKADEMICKIE CENTRUM POLITYKI CYBERBEZPIECZEŃSTWA

SPRAWDŹ KOLEJNE SPOTKANIA:
https://sdsi.pl/webinaria

CYFROWA POLSKA

AKADEMICKIE CENTRUM POLITYKI CYBERBEZPIECZEŃSTWA
ACPC
AKADEMIA SZTUKI WOJENNEJ

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

ZAPROSZENIE
NA KONFERENCJĘ

organizowaną z okazji
Światowego Dnia Społeczeństwa Informacyjnego

POLSKA W TECHNOSFERZE PRZYSZŁOŚCI

PRZEŁOMOWE TECHNOLOGIE TELEINFORMATYCZNE

11 maja 2022 r.

Centrum Nauki Kopernik, godz. 9:30-14:30

wstęp wolny po rejestracji na stronie
www.sdsi.pl/konferencja

SDSI

www.sdsi.pl

Sektorowa Rada ds. Kompetencji
Telekomunikacja i Cyberbezpieczeństwo

ICDL

PTI
POLSKIE TOWARZYSTWO INFORMATYCZNE

Sektorowa Rada ds. Kompetencji
Informatyka