Piotr Markowski

IV Konferencja Naukowa Bezpieczeństwo w Internecie pt. *Cloud Computing – przetwarzanie w chmurze*

Gdy obserwuje się historię rozwoju techniki i technologii, dochodzi się do wniosku, że istnieją dwie podstawowe tendencje ewolucji i przeznaczenia wyrobów będących ich produktami. Najczęściej rozwój techniki i technologii zapoczątkowywany jest w sferze militarnej, ale zdarza się, że i w cywilnej. Mowa tu o cywilnych laboratoriach i ośrodkach naukowych, które wypracowują schematy badawcze wykorzystywane na rzecz obronności i bezpieczeństwa. Nierzadko produkty wstępnie przeznaczone do stosowania tylko w sferze militarnej z upływem czasu znajdują zastosowanie również w życiu codziennym. Dotyczy to w szczególności przypadków zaprzestania wykorzystywania wyrobów powstałych w schematach, o których mowa wyżej, przez zamawiającego albo ich umyślnego lub mimowolnego upowszechniania przez ośrodki naukowo-badawcze i producentów. Przykładami takich wyrobów są produkty uzyskiwane za pomocą technologii produkcji teflonu, mikrofalówek, laserów, silników odrzutowych i systemu GPS.

Zdecydowanie mniej produktów będących wynikiem prac laboratoriów i ośrodków działających poza sferą militarną zastosowano do ochrony bezpieczeństwa oraz w obronności. Przy tym dominowało w tym przypadku ich dostosowywanie do potrzeb sfery militarnej. Wśród technologii można tu wymienić niektóre technologie wykorzystywane w branży energetycznej.

Biorąc pod uwagę wyłącznie technologie komputerowe, a w szczególności techniki sieciowe, w przeważającej liczbie opracowań wskazuje się, że techniki sieciowe zostały opracowane i pierwotnie były wykorzystywane wyłącznie w sferze militarnej. Następnie w drodze ewolucji zostały rozpowszechnione w ośrodkach naukowych, ostatecznie znajdując zastosowanie w życiu codziennym. Techniki sieciowe, w przypadku ich wykorzystywania w wyżej wymienionych sferach, były udoskonalane poprzez zwiększanie liczby i zakresu usług oraz zastosowań. Jednym z przykładów technologii będącej wynikiem udoskonalenia sieci teleinformatycznych jest technologia chmury[1] (z ang. *cloud computing*). W związku z niepodważalnymi zaletami tej technologii, znajdującymi uznanie wśród użytkowników na całym świecie, coraz częściej dostrzega się tendencje zmierzające w kierunku jej wykorzystania w sferze obronności, w tym m.in. w zakresie ochrony informacji niejawnych. W ostatnim okresie można zaobserwować

[1] Pojawienie się usług przetwarzania w chmurze stanowi fundamentalną zmianę w ekonomice informatyki. Technologia chmury normalizuje i tworzy pule zasobów informatycznych oraz automatyzuje wiele zadań utrzymania, które są obecnie wykonywane ręcznie. Architektura chmury ułatwia elastyczne korzystanie, samoobsługę oraz płacenie za zużyte zasoby. Chmura pozwala także na przeniesienie głównej infrastruktury informatycznej do dużych centrów danych, które korzystają ze znacznych oszczędności wynikających ze skali w trzech obszarach:

1) oszczędności po stronie dostawcy (niższe koszty na serwer w dużych centrach danych),
2) agregacja zapotrzebowania. Połączone potrzby prztwarzania wyrównują ogólną zmienność potrzeb, pozwalając na zwiększenie stopnia wykorzystania serwera,
3) efektywność obsługi wielu podmiotów. Przy zmianie na model aplikacji dla wielu użytkowników-zwiększa się liczba korzystajacych z niego podmiotów (np. klientów lub użytkowników), co zmniejsza koszty zarządzania aplikacją i utrzymania serwera na jeden podmiot.

zainteresowanie użytkowników systemów teleinformatycznych (TI), w których są przetwarzane informacje niejawne, zaletami systemów działających w technologii chmury.

Niniejszy artykuł to sprawozdanie z udziału Agencji Bezpieczeństwa Wewnętrznego w konferencji poświęconej wykorzystaniu technologii chmury do przetwarzania danych, w tym także w sferze bezpieczeństwa państwa.

* * *

W dniu 29 maja 2012 r. w auli Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie odbyła się IV konferencja naukowa z cyklu *Bezpieczeństwo w Internecie*, zatytułowana *Cloud computing – przetwarzanie w chmurze*. Tegorocznymi organizatorami konferencji byli: Uniwersytet Kardynała Stefana Wyszyńskiego, Agencja Bezpieczeństwa Wewnętrznego, Generalny Inspektor Ochrony Danych Osobowych i Naukowe Centrum Prawno-Informatyczne. Przedstawiciel ABW przedstawił w panelu zatytułowanym *Władze w chmurach* prezentację pt. *Przetwarzanie danych w chmurze – aspekt informacji niejawnych*.

Prezentacja ABW była ostatnią prezentacją panelu, poprzedzoną wystąpieniami przedstawicieli jednostek naukowych i struktur administracji państwowej mających doświadczenie w zakresie wykorzystania technologii chmury albo zainteresowanych wykorzystaniem tego typu technologii w realizacji niektórych zadań. Jej głównym celem było zwrócenie uwagi uczestników konferencji na właściwe postępowanie z informacjami niejawnymi zawartymi na nośnikach elektronicznych, przetwarzanymi, przechowywanymi i transmitowanymi z wykorzystaniem technologii chmury.

Na wstępie prezentacji przedstawiono aktualne akty prawne dotyczące przetwarzania informacji niejawnych w systemach teleinformatycznych oraz rolę Agencji Bezpieczeństwa Wewnętrznego w procesie ich ochrony. Wśród wskazanych przepisów znalazły się w szczególności:

1. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r. Nr 182, poz. 1228),
2. *Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego* (Dz.U. z 2011 r. Nr 159, poz. 948),
3. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (DZ.U. z 2010 r. Nr 29, poz. 154),
4. *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Dz.U. z 1997 r. Nr 88, poz. 553 z późn. zm.).

W celu podkreślenia, że wymagania dotyczące bezpieczeństwa informacji niejawnych i ich właściwa ochrona wynikają z przepisów prawa, w prezentacji posłużono się bezpośrednimi odwołaniami do konkretnych zapisów. Jednocześnie zaznaczono, że rola ABW w tym zakresie została określona bardzo precyzyjnie, a działania podejmowane przez Agencję są zgodne z obowiązującym prawem.

Prezentacja ABW była podzielona na dwie części: pierwszą – informacyjną – dotyczącą zasad ochrony informacji niejawnych, w tym skutków nieprawidłowego ich stosowania, i drugą – dotyczącą trudności, jakie mogą napotkać kierownicy jednostek organizacyjnych przewidujący przetwarzanie danych w chmurze. Poniżej przedstawiono najważniejsze fragmenty prezentacji.

Na wstępie części pierwszej zdefiniowano informacje niejawne:

Informacje niejawne (IN) – informacje wymagające ochrony przed ich nieuprawnionym ujawnieniem, które spowodowałoby lub mogłoby spowodować szkody dla

Rzeczypospolitej Polskiej albo byłoby niekorzystne z punktu widzenia jej interesów, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania – art. 1 ust. 1 UOIN:.

Podczas prezentacji zwrócono uwagę na podstawowe cechy informacji niejawnych, tj. na to, że są to informacje prawnie chronione, że ich nieuprawnione ujawnienie powoduje określony skutek i że mogą być wyrażane w różnych formach. Wskazano też, że niezależnie od formy i sposobu wyrażania informacje niejawne zostały podzielone zgodnie z wpływem skutków ich nieuprawnionego ujawnienia na interesy RP i jej obywateli. Odniesiono się do wszystkich klauzul tajności i krótko je zdefiniowano. Szczególnie zwrócono uwagę na brak podziału informacji niejawnych w najnowszej ustawie na informacje stanowiące tajemnicę państwową i służbową. Podkreślono również szczególną rolę kierowników jednostek organizacyjnych odpowiedzialnych za właściwe zabezpieczanie tego typu informacji.

Kolejnym etapem tej części było przedstawienie zadań, jakie polski ustawodawca postawił przed ABW, określając jej właściwość rzeczową wynikającą z art. 5 ustawy o ABW oraz AW, tj. :

(…) *realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych.*

W prezentacji doprecyzowano zadania ABW dotyczące bezpieczeństwa wykorzystania systemów TI przetwarzających informacje niejawne. Do zadań tych należą:

1) akredytacja systemów teleinformatycznych (od klauzuli „poufne" wzwyż) – art. 48 UOIN,
2) certyfikacja – art. 50 UOIN:
   a) urządzeń i narzędzi ochrony kryptograficznej,
   b) urządzeń i narzędzi służących do zabezpieczenia teleinformatycznego,
   c) środków ochrony elektromagnetycznej.
4) Przeprowadzanie szkoleń administratorów i inspektorów bezpieczeństwa teleinformatycznego,
5) Przeprowadzanie kontroli bezpieczeństwa przetwarzania informacji niejawnych w systemach TI – art. 52 UOIN.

Na kolejnych etapach części pierwszej szczegółowo omówiono odpowiedzialność osób przetwarzających informacje niejawne w sposób niewłaściwy, ze wskazaniem na poniższe artykuły kodeksu karnego (rozdział XXXIII):

– art. 265 kk:

§ 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje o klauzuli „tajne" lub „ściśle tajne", podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Z uwagi na to, że znaczną część audytorium konferencji stanowili funkcjonariusze publiczni instytucji i podmiotów zewnętrznych, w prezentacji ABW wskazano na szczególną odpowiedzialność tej grupy osób za właściwe przetwarzanie informacji niejawnych.

– art. 266 § 2 kk:

Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację o klauzuli „zastrzeżone" lub „poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

Funkcjonariuszem publicznym w rozumieniu art. 115 § 13 kk jest**:**

1) Prezydent Rzeczpospolitej Polskiej,
2) poseł, senator, radny,
3) sędzia, ławnik, prokurator, funkcjonariusz finansowego organu postepowania przygotowawczego lub organu nadrzędnego nad finansowym organem postępowania przygotowawczego, notariusz, komornik, kurator sądowy, syndyk, nadzorca sądowy i zarządca, osoba orzekająca w sprawach o wykroczenia lub w organach dyscyplinarnych działających na podstawie ustawy,
4) osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych,
5) osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe,
6) osoba zajmująca kierownicze stanowisko w innej instytucji państwowej,
7) funkcjonariusz organu powołanego do ochrony bezpieczeństwa publicznego albo funkcjonariusz Służby Więziennej,
8) osoba pełniąca czynną służbę wojskową,
9) pracownik międzynarodowego trybunału karnego, chyba że pełni wyłącznie czynności usługowe.

W drugiej części prezentacji przedstawiono niektóre wymagania dotyczące ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych działających w technologii chmury, których spełnienie jest obligatoryjne przy uzyskiwaniu świadectwa akredytacji systemu teleinformatycznego upoważniającego do przetwarzania informacji niejawnych lub do uzyskania pozytywnej oceny bezpieczeństwa systemu teleinformatycznego o klauzuli „zastrzeżone". Przewidywane rodzaje problemów związane z przetwarzaniem informacji niejawnych w systemie TI działającym w technologii chmury zobrazowano w poniższej tabeli.

Informacje niejawne – niektóre wymagania	**Przetwarzanie w chmurze – uwagi i problemy**
ODPOWIEDZIALNOŚĆ	
Art. 14 UOIN: *Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.* **Art. 48 ust. 10 UOIN** *W przypadku gdy system, o którym mowa w ust. 9* [system TI do klauzuli „zastrzeżone" – przyp. aut. art.]*, będzie funkcjonował w więcej niż jednej jednostce organizacyjnej, akredytacji, o której mowa w ust. 9, udziela kierownik jednostki organizującej system.*	1. Odpowiedzialność za ochronę informacji niejawnych przetwarzanych w chmurze jest rozłożona na wiele podmiotów. 2. Informacje są przetwarzane w systemach TI należących do wielu podmiotów zapewniających różną politykę bezpieczeństwa, często zależnych od lokalnego prawa. 3. Kwestia odpowiedzialności prawnej za ochronę informacji niejawnych jednego kraju na terytorium innego jest nierozstrzygnięta (niejednoznaczność i niespójność przepisów prawa). 4. Możliwość zdeponowania informacji niejawnych u usługodawców (właścicieli chmury) na czas ich przetwarzania w chmurze.

OBSZAR PRZETWARZANIA INFORMACJI NIEJAWNYCH	
Art. 49 UOIN: *1. Kierownik jednostki organizacyjnej jest odpowiedzialny za wyznaczenie obszarów wytwarzania, przetwarzania i przechowywania informacji niejawnych (szacowanie ryzyka).* *2. Systemy TI dedykowane do przetwarzania informacji niejawnych są szczegółowo zdefiniowane w dokumentacji bezpieczeństwa (SWBS i PBE) zatwierdzanej przez ABW lub SKW.* *3. Systemy TI muszą być akredytowane przez ABW lub SKW, a od klauzuli „poufne" wyżej także audytowane.* *4. Systemy TI przetwarzające informacje do klauzuli „zastrzeżone" są akredytowane do przetwarzania informacji niejawnych przez kierownika jednostki organizacyjnej. Dokumentacja bezpieczeństwa jest oceniana przez ABW lub SKW.* *5. Dokonywanie jakichkolwiek zmian w systemie TI jest dopuszczalne wyłącznie na zasadach opisanych w UOIN (szacowanie ryzyka).*	1. Utrudnione, a w niektórych przypadkach wręcz niemożliwe, jest precyzyjne wskazanie obszarów, w których sa przechowywane informacje niejawne. Rozproszenie usług, sprzętu, nośników danych, będące zaletami dla technologii chmury, nie idzie w parze z wymaganiami dotyczącymi informacji niejawnych w zakresie pełnej wiedzy o obszarze przetwarzania. 2. Systemy TI działające w technologii chmury są systemami podlegającymi częstym modyfikacjom, często dokonywanym bez wiedzy właściciela danych. 3. Zalety systemów działających w technologii chmury, takie jak elastyczność, skalowalność, szybka reakcja na potrzeby zmian i dostosowanie się do potrzeb wszystkich klientów, mogą stanowić problem dla przetwarzania informacji niejawnych.
OCHRONA FIZYCZNA	
Art. 45 ust. 1 UOIN: *Jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności chroniące przed:* *1) działaniem obcych służb specjalnych;* *2) zamachem terrorystycznym lub sabotażem;* *3) kradzieżą lub zniszczeniem materiału;* *4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;* *5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.* **Art. 46 UOIN:** *W celu uniemożliwienia osobom nieuprawnionym dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej należy w szczególności:* *1) zorganizować strefy ochronne;* *2) wprowadzić system kontroli wejść i wyjść ze stref ochronnych;* *3) określić uprawnienia do przebywania w strefach ochronnych;* *4) stosować wyposażenie i urzadzenia służące ochronie informacji niejawnych, którym przyznano certyfikaty.*	1. Ochrona fizyczna systemu TI (który z zasady może być wirtualny) działającego w technologii chmury jest trudna w realizacji. 2. Przetwarzanie informacji w systemach, których strefy ochronne znajdują się w lokalizacjach, w których obowiązuje inna polityka bezpieczeństwa i różne przepisy prawa w zależności od lokalizacji sytemu TI w chmurze, wiąże się z trudnościami poza-technicznymi, związanymi z rozstrzygnięciami prawnymi. Przykładem jest wymóg ochrony informacji niejawnych przed działaniem obcych służb specjalnych poza terytorium kraju, w lokalizacjach niepodległych kierownikowi jednostki organizującej system TI.

PRZETWARZANIE POZA STREFAMI OCHRONNYMI	
§ 10. ust 2 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r.*: *Poufność informacji niejawnych przekazywanych w formie transmisji poza strefami ochronnymi zapewnia się przez stosowanie urządzeń lub narzędzi kryptograficznych, certyfikowanych zgodnie z art. 50 ust. 2 UOIN lub dopuszczonych w trybie art. 50 ust. 7 UOIN, odpowiednich do klauzuli tajności przekazywanych informacji*.	1. Obecnie istniejące systemy teleinformatyczne działające w technologii chmury nie są wyposażone w środki ochrony kryptograficznej, certyfikowane zgodnie z UOIN. 2. Stosowanie odpowiednich środków ochrony utrudniają: rozproszenie sieci, dynamika zmian systemów w chmurze, potrzeba wysokiej wydajności oraz różne przepisy prawa w zależności od lokalizacji systemu.
INTEGRALNOŚĆ DANYCH	
1. Zabezpieczenia stosowane w systemie TI muszą zapewnić poufność, integralność i dostępność przetwarzania informacji niejawnych. 2. Środki ochrony integralności informacji w systemach TI przetwarzających informacje niejawne muszą być certyfikowane (art. 50 ust.3 UOIN). 3. Środki ochrony integralności informacji muszą zapewnić integralność danych na każdym etapie, od momentu wytworzenia do usunięcia.	1. Mechanizmy integralności informacji w chmurze są różnorodne, poziom ochrony nie jest jednolity. 2. Brak informacji o występowaniu środków ochrony integralności w systemach teleinformatycznych działających w technologii chmury, certyfikowanych przez ABW lub SKW.
OBIEG INFORMACJI, KOPIOWANIE, UDOSTĘPNIANIE	
Art. 4 UOIN: *Kierownik jednostki organizacyjnej odpowiedzialny za ochronę IN organizuje obieg IN, który uwzględnia:* *1. Wytwarzanie,* *2. Rejestrowanie,* *3. Przechowywanie,* *4. Kopiowanie,* *5. Usuwanie (niszczenie) IN.* *Obieg IN zapewnia rozliczalność IN, także zapoznanie i udostępnianie IN (niezależnie od formy wyrażenia).*	Ze względu na cechy systemów TI wykonanych w technologii chmury, takie jak: skalowalność, szybka reakcja na potrzeby zmian, elastyczność i szeroka dostępność, obieg informacji uwzględniający jedną, wspólną politykę bezpieczeństwa, jest trudny do zrealizowania ze względów technicznych i prawnych. Rozproszenie informacji w chmurze utrudnia zastosowanie zasad ograniczających ich nieuprawnione kopiowanie i usuwanie oraz dostęp do nich.
USUWANIE INFORMACJI Z SYSTEMU TI	
1. *Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r.* określa zasady usuwania informacji niejawnych, ich niszczenia i deklasyfikacji, 2. Informacje niejawne po wykorzystaniu powinny zostać trwale usunięte, 3. Przepisy prawa wymuszają klasyfikowanie komponentów systemu TI, które zawierają informacje niejawne, 4. § 17 ust. 4 *Rozporządzenia*: dopuszcza się deklasyfikowanie nośników i ich niszczenie po wykorzystaniu (poniżej klauzuli „tajne"). 5. Wymagane są odpowiednie procedury bezpiecznej eksploatacji odnośnie do usług serwisowych i niszczenia lub utylizacji komponentów technicznych systemu TI.	Dane w chmurze są rozproszone, a ich położenie i liczba mogą się zmieniać w zależności od potrzeb i dostępności miejsca w chmurze (liczba nośników). Trudno wskazać skuteczne metody usuwania określonej informacji (dokumentu) z chmury. Istnieje wysokie ryzyko pozostawania danych na nośnikach.

Ze względu na ograniczenia czasowe podczas prezentacji przedstawiono wyłącznie podstawowe wymagania dotyczące systemów TI przetwarzających informacje niejawne. Poinformowano audytorium, że prezentacja nie wyczerpuje całości zagadnienia. Zaznaczono, że nie objęła ona m.in. kwestii dostępu do informacji niejawnych

poszczególnych osób oraz wymagań dotyczących ochrony elektromagnetycznej (stref sprzętowej ochrony elektromagnetycznej, urządzeń klasy TEMPEST[2]).

Podsumowując prezentację ABW, można uznać, że wobec zbyt optymistycznego podejścia do przetwarzania danych instytucji państwowych w systemach TI w technologii chmury zwróciła ona uwagę uczestników konferencji na wiele problemów z tym związanych. Z rozmów przeprowadzonych podczas konferencji wynikało, że niektórzy gestorzy systemów TI nie są w pełni świadomi wymagań technicznych, prawnych i organizacyjno-proceduralnych wynikających z przepisów, których spełnienie jest niezbędne do przetwarzania informacji niejawnych. W związku z powyższym nasunął się wniosek, że niezbędne jest poszerzanie wiedzy dotyczącej ochrony informacji niejawnych na przykład poprzez organizowanie przez funkcjonariuszy ABW szkoleń m.in. dla administratorów i inspektorów bezpieczeństwa teleinformatycznego.

W podsumowaniu prezentacji potwierdzono, że ABW, jako organ wyposażony w szczególne prawa i obowiązki w zakresie ochrony informacji niejawnych, dostrzega możliwość przetwarzania tego typu danych w systemach TI wykonanych i działających w technologii chmury tylko w przypadku spełniania przez te systemy wszystkich wymagań niezbędnych do ochrony takich informacji.

[2] Norma TEMPEST (*Temporary Emanation and Spurious Transmission*), ustanowiona w Stanach Zjednoczonych na zlecenie Pentagonu, jest sposobem zabezpieczania przed niekontrolowaną emisją promieniowania elektromagnetycznego, generowanego przez rozmaite urządzenia, w tym komputery (norma ta powstała w latach 50.). Promieniowanie takie może być wykorzystywane przy użyciu specjalnych urządzeń odbiorczych do „podsłuchiwania" pracujących komputerów. Stosowanie sprzętu klasy TEMPEST gwarantuje bezpieczeństwo procesu przetwarzania danych i wyklucza możliwość przechwytywania poufnych informacji. Ze względu na szczególną wagę dla bezpieczeństwa państwa zarówno normy, jak i technologia TEMPEST, są utajnione.