

Elektromagnetyczna apokalipsa... E- bomby: nowa odmiana terroryzmu?

Autor: Piotr Olszowiec

(„Energia Gigawat”- nr 12/2011)

Powszechne stosowanie urządzeń elektronicznych i mikroprocesorowych uczyniło naszą cywilizację podatną na nowe zagrożenia. Liczne elementy elektryczne, a zwłaszcza elektroniczne są bardzo wrażliwe na przepięcia (tj. nadmiernie wysokie napięcia) przenoszone do obwodów przez sprzężenia indukcyjne lub pojemnościowe bądź przez miejsca uszkodzenia izolacji.

Dla przeniknięcia fali przepięciowej do układu elektrycznego po przewodach linii konieczne jest przekroczenie zdolności pochłaniania energii zainstalowanych w nim elementów ochronnych. Uszkodzenie układów elektronicznych może spowodować impuls prądu elektrycznego o odpowiednio wysokim napięciu i energii mniejszej od milidżuła (10^{-3} J), przy czym czas jego trwania nie musi przekraczać mikrosekundy (10^{-6} s). Typowe ochronniki przepięciowe wykazują wprawdzie zdolność pochłaniania impulsów o wielokrotnie większej energii, lecz ich stosowanie nie jest ograniczone z powodu wysokiej ceny. Przepięcia w obwodach elektrycznych wywołują także przenikające je zewnętrzne, zmienne pola magnetyczne. Dotychczas uważano, że układy elektroniczne umieszczone w metalowej obudowie są skutecznie zabezpieczone przed działaniem zewnętrznych pól elektromagnetycznych. Jednak badania wykazały, że nawet metalowa klatka Faradaya nie w pełni chroni aparaty przed wnikaniem impulsów fal elektromagnetycznych wielkiej częstotliwości. Źródłem impulsowych pól mogą być np. wyładowania atmosferyczne, zjawiska w układach wysokich napięć, eksplozje nuklearne lub użycie innych rodzajów broni zwanych skrótowo e-bombami.

Badania nad e-bombą zapoczątkował w sposób niezamierzony w 1925 r. A. Compton, który odkrył zjawisko nazwane później jego imieniem. Strumień fotonów uderzających w atomy pierwiastków o niskiej liczbie atomowej wywołuje emisję elektronów. Już pierwsze wybuchy atomowe ujawniły niszczycielską siłę wygenerowanego pola elektromagnetycznego. W 1958 r. przeprowadzono wybuch bomby wodorowej w atmosferze nad Pacyfikiem. Wytworzone promieniowanie gamma wywołało emisję elektronów z atomów tlenu i azotu. Strumienie elektronów dotarły na Hawaje, powodując tam awarie sieci oświetleniowej, zaś w Australii - zakłócenia łączności radiowej. Od tamtej pory trwa wyścig w doskonaleniu broni elektromagnetycznych oraz sposobów ochrony przed ich działaniem. Jednym z wynalazków, opracowanym przed pół wiekiem w Los Alamos, był generator z tzw. wybuchową kompresją pola magnetycznego. Bomba ta zawiera rurę z materiałem wybuchowym, umieszczoną wewnątrz cewki indukcyjnej. Bezpośrednio przed zdetonowaniem materiału cewka zostaje zasilona z naładowanej baterii kondensatorów, wskutek czego wytwarza silne pole magnetyczne. Płonące gazy powstałe z eksplozji materiału przemieszczają się przez cewkę, zwińcując jej kolejne zwoje. W trakcie propagacji zwarcia pole magnetyczne ulega swoistej kompresji („sprężaniu”). W rezultacie w zwojach cewki powstaje stromo narastający impuls prądu, który znika w chwili ostatecznego zniszczenia cewki. Czas narastania impulsu trwa zaledwie ułamek mikrosekundy, a wartość szczytowa prądu przekracza dziesiątki milionów amperów. Impuls fali elektromagnetycznej o ogromnej sile rażenia zostaje wypromieniowany przez antenę do otoczenia.

Inny rodzaj e-bomby stanowi generator fal elektromagnetycznych z „wirtualną” katodą, zrealizowany na bazie lampy elektronowej zwanej „wirkatorem”. Po przyłożeniu do anody dodatniego potencjału rzędu miliona woltów, z katody emitowany jest strumień elektronów. Po przejściu przez siatkę anody ruch tych elektronów ulega wyhamowaniu przez przyciąganie anody, co jest równoważne odpychaniu przez „wirtualną” katodę – stąd nazwa lampy. Po wycofaniu przez siatkę anody elektrony są teraz odpychane przez rzeczywistą katodę. W rezultacie następują oscylacje obłoku elektronowego między rzeczywistą i „wirtualną” katodą. Powstające pole elektromagnetyczne bardzo wysokiej częstotliwości jest emitowane do otoczenia lampy przez jej antenę. Natężenie prądu (czyli strumienia elektronów w lampie) sięga 1-10 kA, co przy napięciu rzędu MV daje szczytową moc chwilową impulsu (trwającego wprawdzie zaledwie nanosekundy) blisko 40 GW! Nowoczesne e-bomby po udanych próbach w wojnie w Zatoce Perskiej 1990 r. włączono do arsenałów armii niektórych krajów. Przykładem jest generator impulsów promieniowania elektromagnetycznego - amerykańskie urządzenie typu MPS-II - przeznaczony do niszczenia systemów informatycznych i elektronicznych przeciwnika. Wykorzystano w nim źródło fal z lustrzaną anteną o średnicy 3 m, z której wysyłany jest strumień o mocy chwilowej ok. 1 GW, wytwarzany przez oscylacje prądu o maksymalnych wartościach 3.5 kA i 265 kV. Strefa rażenia przez to „śmiercionośne” lustro obejmuje sektor o kącie środkowym 24 stopnie i promieniu 800 m. Emitowane fale uszkadzają w tej strefie wszelkie układy elektroniczne i komputerowe, w tym także nośniki magnetyczne jak rozmaite karty oraz m.in. rozruszniki serca. Dotychczas opracowano i przebadano wiele technologii broni elektromagnetycznych. Zalicza się do nich m.in. magnetrony, klistrony, żyrotrony, lasery na wolnych elektronach, generatory plazmowe i wspomniane wirkatory.

Niestety podobnymi broniąmi dysponują prawdopodobnie również organizacje terrorystyczne. Dla konstrukcji środków elektromagnetycznego rażenia wykorzystują one m.in. wycofywane, przestarzałe urządzenia radarowe działające w paśmie częstotliwości do 5 GHz. Źródła takie można instalować na samochodzie, zaś ich miniaturowe wersje można przenosić nawet w ... walizce. Egzemplarze „walizkowe” są dostępne za pośrednictwem Internetu w cenie od 100 000 USD. Jednak podobną zdolność rażenia terroryści mogą uzyskać tańszym kosztem, nawet za kilkaset dolarów. Eksperci oceniają, że organizacja dysponująca techniką sprzed pół wieku jest w stanie skonstruować samodzielnie niektóre e-bomby. Nawet te najmniejsze przenośne promienniki są w stanie skutecznie zakłócić pracę wszelkich układów elektrycznych, telekomunikacyjnych i informatycznych w obiektach oddalonych o 500-1000 m. Dla osiągnięcia zamierzonej skali rażenia e-bombę wystarczy zdetonować w dość znacznej odległości od celu, na przykład na dużej wysokości nad miastem. Atak ten może w pierwszej chwili zostać w ogóle niezauważony, jako że nie towarzyszy mu żaden huk, dym czy ogień. Wkrótce jednak w najbliższej strefie następuje wyłączenie, uszkodzenie lub wręcz fizyczne zniszczenie wszelkiej aparatury i urządzeń elektrycznych, elektronicznych i komputerowych. Życie w dotkniętym obszarze ulega całkowitemu „paraliżowi” – gasną światła, telewizory, komputery, zatrzymują się pojazdy, pociągi, dopływ wody, klimatyzacja itd. W miarę upływu czasu zasięg strefy rażenia stopniowo rozszerza się – proroczą wizję takiego kataklizmu przedstawia widok e-bomby zdetonowanej nad miastem.

Celem takiej hipotetycznej zagłady cywilizacji technicznej mogą stać się w pierwszym rzędzie obiekty energetyki, która decyduje o normalnym funkcjonowaniu gospodarki i życiu ludności. Niestety stosowane tu coraz powszechniej mikroprocesorowe urządzenia sterowania i zabezpieczeń są nieporównanie bardziej podatne na zakłócenia elektryczne i elektromagnetyczne niż ich poprzednie generacje elektromechaniczne lub nawet

elektroniczne. Dla uodpornienia tych układów na powyższe zagrożenia należy jak najszybciej opracować i wdrażać skuteczne środki zaradcze. Przykładowe, sprawdzone już rozwiązania, obejmują między innymi:

- zupełną wymianę wszystkich połączeń przewodowych do urządzeń cyfrowych (wraz z obwodami wtórnymi prądowymi i napięciowymi) na włókna światłowodowe,
- użycie optoelektronicznych przekładników prądowych i napięciowych nowej generacji w miejsce tradycyjnych przekładników rdzeniowych,
- wprowadzenie pełnej galwanicznej separacji od sieci elektrycznej i zasilanie obwodów pomocniczych ze źródeł autonomicznych,
- umieszczenie mikroprocesorowych aparatów w szczelnych metalowych szafach wykonanych w specjalnej technologii zapewniającej nieprzenikalność dla fal elektromagnetycznych najwyższych częstotliwości.

Nie ulega wątpliwości, że te złożone rozwiązania okażą się bardzo wysoką ceną za zapewnienie bezpieczeństwa energetycznego naszej cywilizacji w dobie terrorystycznych zagrożeń. Niestety koszt ten został bardzo wyśrubowany przez trwającą od dwóch dekad rewolucję informatyczną w przemysłowych systemach automatyki, sterowania i zabezpieczeń.