ZAŁĄCZNIK NR 2
ZAGROŻENIA ZWIĄZANE Z KORZYSTANIEM Z USŁUG ŚWIADCZONYCH DROGĄ ELEKTRONICZNĄ

1. Możliwość otrzymania spamu, czyli niezamówionej informacji reklamowej (handlowej) przekazywane drogą elektroniczną.
2. Działanie oprogramowania typu malware, czyli oprogramowania, które jest w stanie, po uruchomieniu, zarazić pliki w sposób samopowielający, zazwyczaj nie będąc zauważonym przez użytkownika. Wirusy komputerowe mogą być mniej lub bardziej szkodliwe dla systemu operacyjnego, w którym się znajdują, ale nawet w najmniej poważnym przypadku są marnotrawstwem pamięci RAM, CPU i miejsca na twardym dysku.
3. Obecność i działanie robaków internetowych (worm), czyli szkodliwego oprogramowania zdolnego do samopowielania. E-mail worm jest niszczącym atakiem przeciwko sieci, polegającym na zebraniu wszystkich adresów e-mail znajdujących się w lokalnym programie (na przykład w MS Outlook) i wysłaniu na nie setek e-maili zawierających robaka w niewidocznym załączniku.
4. Możliwość zadziałania oprogramowania typu spyware, to jest oprogramowania szpiegującego działania użytkownika w Internecie, instalującego się bez jego wiedzy, zgody i kontroli.
5. Możliwość bycia narażonym na cracking lub phishing (łowienie haseł) - w kontekście informatycznym phishing oznacza technikę łamania zabezpieczeń (cracking), używaną do pozyskania osobistych i poufnych informacji w celu kradzieży tożsamości, poprzez wysyłanie fałszywych wiadomości elektronicznych przypominających do złudzenia autentyczne.
6. Piractwo komputerowe - termin używany przez piratów komputerowych do określenia oprogramowania, z którego zdjęto zabezpieczenie przed kopiowaniem i które udostępniono w Internecie, skąd może być pobrane
7. Sniffing - niedozwolony podsłuch, inny niż mieszczący się w granicach pojęcia cracking i phising, polegający na wykorzystaniu sniffera - programu komputerowego, którego zadaniem jest przechwytywanie i ewentualne analizowanie danych przepływających w sieci
8. Możliwość wprowadzenia przez inne osoby korzystające z systemu teleinformatycznego i/lub sieci telekomunikacyjnej nielegalnych urządzeń dających nieuprawniony dostęp do usług podlegających ochronie,
9. Kryptoanaliza, to jest odnalezienia słabości systemu kryptograficznego, a tym samym umożliwienia jego złamania lub obejścia,
10. Możliwość bycia narażonym na działania innego niechcianego lub "złośliwego" oprogramowana, wykonującego czynności niezamierzone przez użytkownika, niewchodzące w granice definicji wymienionych powyżej, a występujace pod nazwami: wabbit, trojan, backdoor, exploit, rootkit, keylogger, dialer, hoax.