

V současné době je vládní návrh trestního zákoníku (sněmovní tisk č. 744/0) ve fázi druhého čtení. Ústavně právní výbor projednal návrh zákona a vydal 2. 5. 2005 usnesení doručené poslancům jako tisk 744/1 obsahující *pozměňovací návrhy*. Projednávání tisku 744/1 je na pořadu 47. schůze (od 20. 9. 2005).

## **Názor odborníků z oblasti ochrany informačních systémů k upřesnění návrhu trestního zákoníku**

Jsme znepokojeni návrhem znění ust. § 204 - 206 trestního zákoníku (sněmovní tisk č. 744/1), který má být projednáván na pořadu 47. schůze Poslanecké sněmovny Parlamentu ČR od 20. 9. 2005.

Podle našeho názoru jsou v současném znění nedostatečně rozlišeny oprávněné a neoprávněné činnosti v oblasti, která se nás pracovně dotýká.

Smyslem prezentace tohoto názoru je předejít možnosti nejednotné interpretace práva při užití zvláště gramatického výkladu. Účelem rekodifikace zákona, resp. definování skutkových podstat nových trestných činů jistě není kriminalizace kryptoanalytických prací vědeckých pracovníků nebo oprávněného testování bezpečnosti počítačových systémů. Současně si dovoluujeme podotknout, že takové oprávnění může spočívat i na smluvním základě.

Zejména by mělo být z dikce zákona zcela dovoditelné, že následující činnosti jsou zákonné:

1. Výuka moderních metod kryptoanalýzy na vysokých školách a univerzitách.
2. Vědecký příspěvek na mezinárodní konferenci.
3. Vědecký názor na odborném internetovém fóru, webu, poštovní konferenci, diskusní skupině.
4. Soukromé e-maily s kryptology diskutující kryptoanalytické metody.
5. Účast ve veřejných mezinárodních soutěžích na prolomení kryptografického algoritmu; poznamenejme, že za tyto činnosti jsou vypsány značné finanční odměny.

Dále nám jde speciálně o úpravu těchto oblastí

### **Kryptoanalýza**

Moderní kryptoanalýza je věda o hledání slabín nebo prolamování matematických metod informační bezpečnosti. Na druhé straně je její výsledek **možné chápat a využít jako návod na zneužití rozpoznaných slabín ke skutečně nezákonné činnosti**. Mezi těmito dvěma póly je velmi citlivá hranice. Trestní zákoník by měl být upraven tak, aby nebyly žádné pochyby o tom, že je umožněna svoboda slova a svobodná výměna idejí v této vědě.

### **Penetrační testování**

Penetrační testování je praktická činnost, objednaná vlastníkem informačního systému k odhalení bezpečnostních slabín systému, kdy jsou dodavatelem prováděny také **činnosti, které se z technického hlediska neodlišují od nezákonných činností** proti tomuto systému. I zde je velmi citlivá hranice mezi oprávněností a neoprávněností. Určitou formou penetračního testování je i odborná činnost administrátorů počítačových sítí, kteří používají nástroje k odhalování slabých hesel uživatelů, a to s cílem je vyloučit z použití, nikoli je zneužít. Dále je to činnost vývojářů, kteří tyto prostředky tvoří. Podobných činností je více a nelze je vyjmenovat. I zde by trestní zákoník měl být upraven tak, aby nebyly žádné pochyby o tom, že tyto činnosti jsou oprávněné a zákonné.

Na důkaz svého souhlasu s tímto Názorem připojuji svůj podpis.

---

RNDr. Vlastimil Klíma,  
nezávislý český kryptolog  
člen mezinárodní organizace pro kryptologický výzkum IACR  
externí lektor kryptologie Matematicko-fyzikální fakulty Univerzity Karlovy v Praze  
v.klima@volny.cz

---

doc. RNDr. Václav Matyáš, M.Sc., Ph.D.,  
Fakulta informatiky Masarykovy univerzity v Brně  
člen redakční rady časopisu Data Security Management  
matyas@fi.muni.cz

---

doc. RNDr. Jiří Tůma, DrSc.,  
vedoucí katedry algebry  
Matematicko-fyzikální fakulta Univerzity Karlovy v Praze  
garant studijního oboru Matematické metody informační bezpečnosti  
tuma@karlin.mff.cuni.cz

---

prof. Ing. Jan Čapek, CSc.  
děkan  
Fakulta ekonomicko-správní  
Univerzita Pardubice  
Studentská 95, 532 10 Pardubice  
Capek@upce.cz

---

JUDr. Ján Matejka  
vědecký pracovník Ústavu státu a práva Akademie věd ČR  
Odborný asistent Právnické fakulty Západočeské univerzity  
matejka@ilaw.cas.cz

---

prof. RNDr. Štefan Porubský, DrSc.,  
Ústav informatiky Akademie věd České republiky  
přednášející informační bezpečnost na Fakultě jaderné a fyzikálně inženýrské  
ČVUT Praha  
Stefan.Porubsky@cs.cas.cz

---

doc. RNDr. Jiří Souček, DrSc.  
učitel na MFF UK, Matematický ústav, oddělení matematického modelování  
učitel na FF UK, Ústav informačních studií a knihovnictví  
jiri.soucek@centrum.cz

---

doc. RNDr. Jan Paseka, CSc.  
KAG PĚF Masarykova univerzita  
garant studijních programů sekce matematika  
člen IQSA, AMS, JČMF  
paseka@math.muni.cz

---

doc. Dr. Ing. Petr Hanáček,  
Fakulta informačních technologií VUT v Brně  
vedoucí Ústavu inteligentních systémů  
hanacek@fit.vutbr.cz

---

doc. Ing. Roman Rak, Ph.D.  
člen katedry Kriministiky Policejní akademie Praha,  
manažer kompetenčního centra vnitropodnikových informačních systémů  
roman.rak@ct.cz

---

Mgr. Pavel Vondruška,  
specialista pro bezpečnost a certifikační služby, ČESKÝ TELECOM a.s.,  
člen mezinárodní organizace pro kryptologický výzkum IACR,  
externí přednášející kryptologie na MFF UK Praha,  
vydavatel odborného internetového e-zinu Crypto-world  
pavel.vondruska@ct.cz

---

Ing. Miroslav Lang  
hlavní konzultant a technický expert společnosti Microsoft pro oblast bezpečnosti,  
kryptologie, PKI, elektronického podpisu a kritérií hodnocení bezpečnosti,  
víceprezident Asociace firem pro ochranu informací,  
člen oficiální oponentní skupiny k Vyhláškám rozpracovávajících zákon o el. podpisu ČR,  
technický expert a poradce pro implementaci el. průkazu občanů v Belgii a Španělsku,  
mirekl@MICROSOFT.com

---

Ing. Jaroslav Pinkava, CSc.,  
ředitel certifikační autority Czechia,  
místopředseda skupiny kryptologie při Jednotě českých matematiků a fyziků,  
jaroslav.pinkava@zoner.cz

---

Ing. Radek Komanický  
ředitel divize Informační bezpečnost  
eBanka a.s.  
rkomanicky@ebanka.cz

---

Ing. Jiří Hejl  
provozní a technický ředitel eIdentity a.s., Akreditovaný poskytovatel kvalifikovaných  
certifikačních služeb  
člen Pracovní skupiny Ministerstva informatiky pro vyhlášku o kvalifikovaných certifikačních  
službách podle zákona č. 227/2000 Sb., o elektronickém podpisu  
jiri.hejl@volny.cz

---

Ing. Daniel Cvrček, Ph.D.  
odborný asistent FIT VUT v Brně, vědecký pracovník FI MU v Brně,  
přednášející kryptografii a bezpečnost na Fakultě podnikatelské VUT v Brně,  
v letech 2003-2004 člen bezpečnostní skupiny University of Cambridge, UK,  
cvrcek@fit.vutbr.cz

---

Ing. Petr Novák

ředitel technologií Smart Card Identification Technologies Group, An ASSA ABLOY Group  
Company  
ředitel SmartWorldAcademy  
člen technického výboru ID WORLD Congress  
petr.novak@cee.acg-id.net

---

Luděk Novák, Ing, PhD., CISA,  
vedoucí konzultant bezpečnosti informací ANECT a.s.,  
člen Rady odborného sdružení ISACA CRC,  
člen technické normalizační komise 20 - Informační technologie,  
novak@isaca.cz

---

RNDr. Antonín Beneš, Ph.D.  
poradce pro technologii a provoz systému SAP ČR, s.r.o.,  
stálý spolupracovník časopisu Data Security Management,  
přednášející informační bezpečnosti na MFF UK v Praze  
antonin.benes@sap.com

---

Dr.rer.nat. Luděk Smolík  
Seculab, s.r.o.  
lsmolik@web.de

---

RNDr. Libor Dostálek,  
konzultant  
Siemens Bussines Services, Praha  
libor.dostalek@siemens.com

---

Mgr. Drahomíra Doležalová,  
vědecký pracovník MFF UK  
redaktorka serveru root.cz  
johanka@ucw.cz

---

RNDr. Eliška Ochodková,  
přednášející informační bezpečnost na katedře informatiky FEI,  
VŠB - Technická univerzita Ostrava  
eliska.ochodkova@vsb.cz

---

Mgr. Jan Janečko  
analytik bezpečnosti IT  
Komerční banka, a. s.  
člen mezinárodní společnosti pro kryptologický výzkum IACR  
jan\_janecko@kb.cz

---

Bc. Ondřej Suchý,  
analytik informační bezpečnosti,  
LOGIOS s.r.o.  
ondrej.suchy@logios.cz

---

Ing. Tomáš Rosa, Ph.D.  
kryptolog,

divize Informační bezpečnost, eBanka, a.s.  
externí lektor kryptoanalýzy Matematicko-fyzikální fakulty Univerzity Karlovy v Praze  
člen mezinárodních organizací IEEE a IACR  
troša@ebanka.cz

---

Podepsáno elektronickým podpisem v období od 13.9. 2005 do 19.9. 2005  
Podklady uschovány u prvního podepsaného