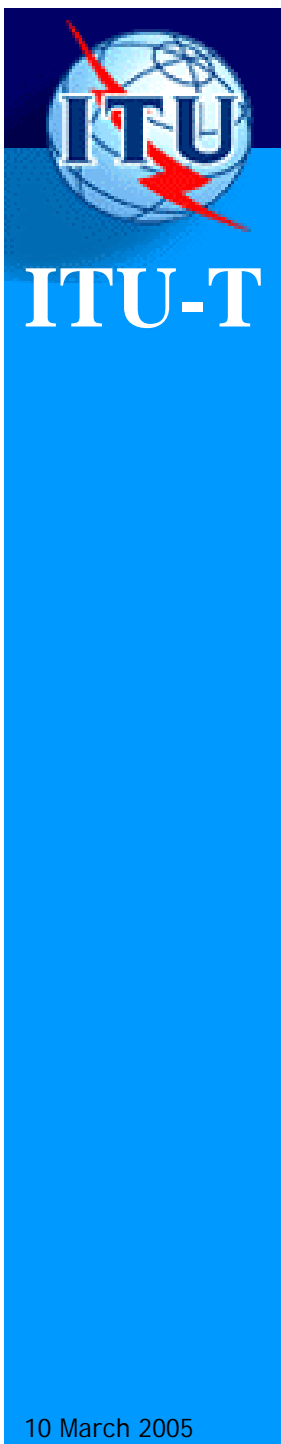




International Telecommunication Union

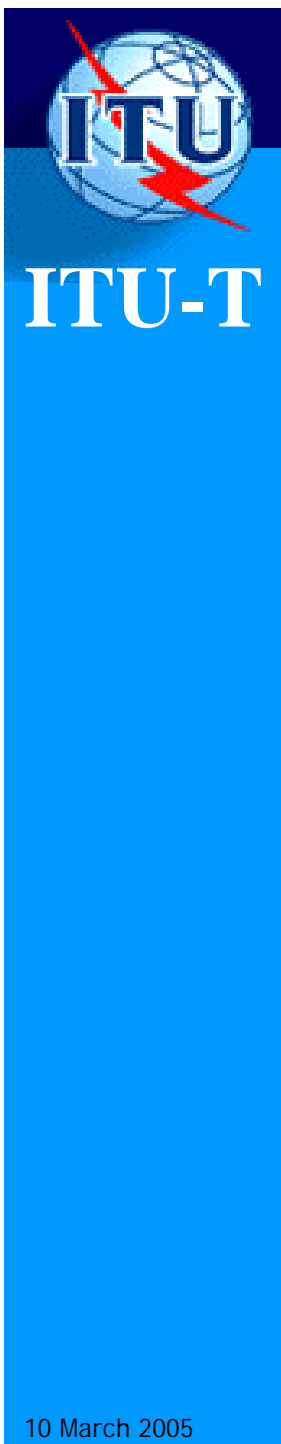
Contemporary threats and integrated approach to information security

Garry Kondakov
Managing Director
Kaspersky Lab
Russia, CIS, and Baltics



Criminalization of Internet

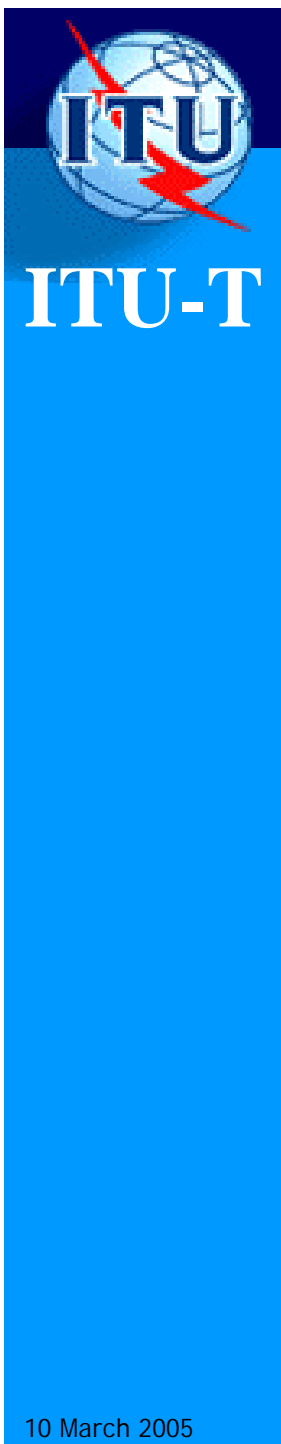
- Hackers and malicious code writers create special networks to support spam dissemination.
- Computer underground is transforming into well-organized criminal groups.
- The number of successful attacks on on-line banks and Internet blackmail (DoS attacks' blackmail) have increased dramatically.
- New types of on-line fraud activities:
 - Phishing;
 - Spyware programs.



Dim reality

- o Material losses of malicious programs:
 - 1995 - 0,5 bill. US\$
 - 1998 - 6,1 bill. US\$
 - 2003 - 13 bill. US\$
 - 2004 - 20 bill. US\$

* - Computer Economics, 2004



Dim reality

- o Material losses of computer viruses 2004:
 - **Sasser** - \$3,5 billion.
 - **NetSky** - \$2,75 billion.
 - **Bagle** - \$1,5 billion.
 - **MyDoom** - \$4,75 billion.

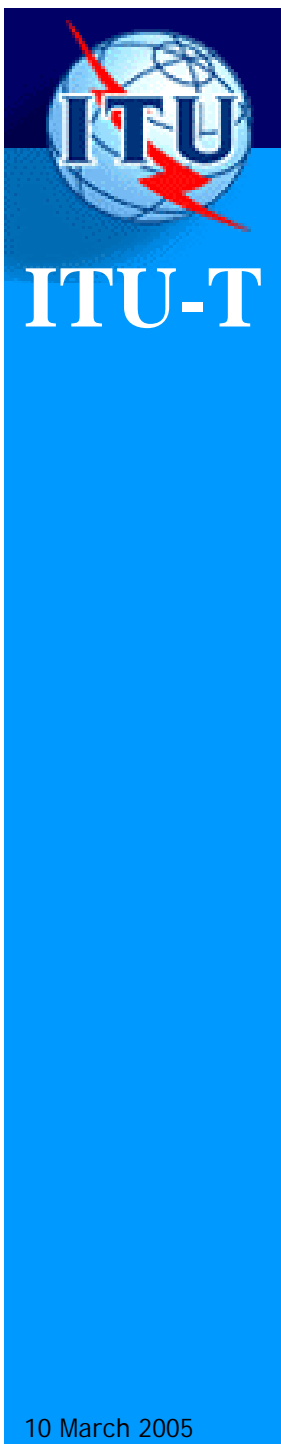
Source: Computer Economics, 2004

- o Spam will cost businesses more than **\$20,5 billion** this year. By the 2007 spam will cost businesses and consumers worldwide over **\$198 billion**.
- o Spam will account for 80 percent of all electronic correspondence by the end of the year

Source: CSO, Forbes

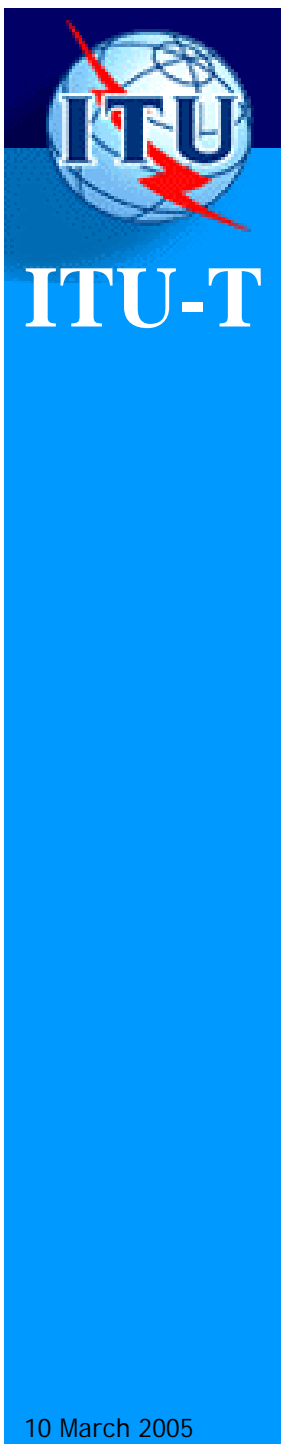
- o Spam costs Russian businesses and consumers over **\$100-150 millions** every year.
- o Spam costs an average of \$50 - \$200 per employee a year in lost productivity

Source: Rambler's social initiative and research fund



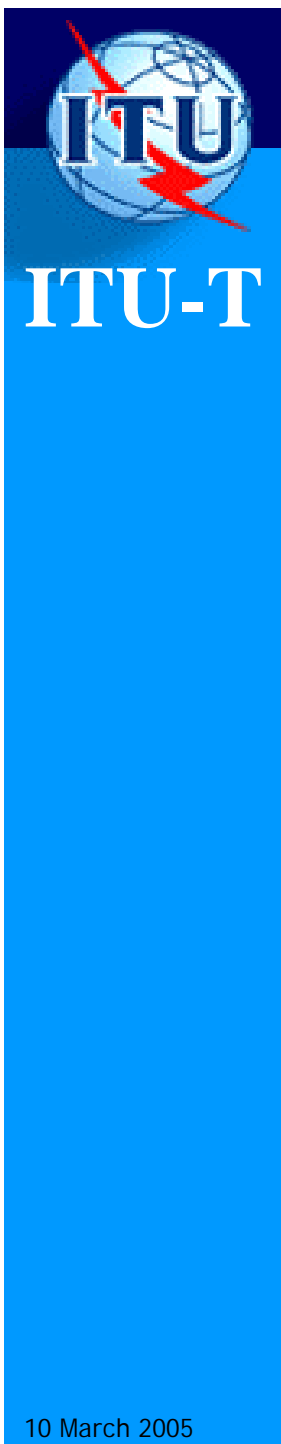
The consequences of the Internet' criminalization

- Creation of well-organized and integrated criminal industries supporting spam, malicious code writing, and hacking.
- The fight against IT threats intensifies dramatically and gets harder.
- “Traditional” criminals use high technologies more frequently and more intensively.
- Potential threat to national and global security.



Today...

- 50% of businesses worldwide do not have information security strategy (Source: LogicaCMG).
- Over 50% of companies do not make sufficient investments in information security (Source: Ernst&Young).
- Over 35% of information networks are vulnerable to external threats (Source: Ernst&Young).
- Less than 30% companies have established information security policies and procedures (Source: Ernst&Young).
- Only 4,8% of all IT spending are associated with information security costs (Source: IDC).



The integrated approach to information security

Four aspects:

- Technology
- Organization
- Government
- International cooperation



The integrated approach to information security

- Business and consumers should use products and solutions based on modern technologies providing protection against ALL types of threats, such as internal threats, viruses, worms, trojans, hackers, spam, etc.
- Business and consumers should use only well-trusted and licensed products and solutions.
- Government and public organizations should use only certified security products.
- Information about computer threats and risks should be delivered to all end users.



The integrated approach to information security

Businesses should work out strategic approach to information security



- Information security strategy, policy, procedures is a must for any serious business and organization.
- Security issues must have the highest priority.
- Modern information security system should be implemented and used to protect business.
- End-users should be informed about the threats associated with the use of modern technologies.

The integrated approach to information security



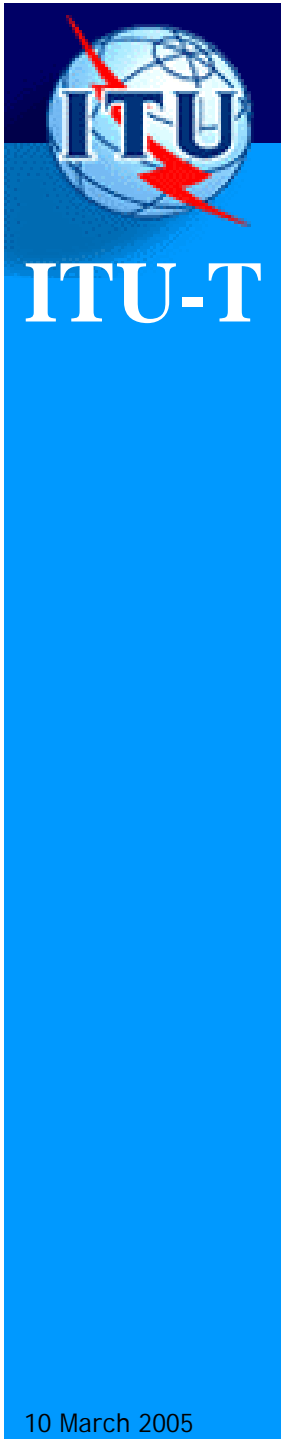
- Laws and regulations, protecting government organizations, businesses, and consumers, should be implemented and tuned to face modern information frauds and crimes.
 - Memorandum on counteracting the dissemination of malicious programs (viruses) and unauthorized advertising messages (spam) (Russian Association for Networks and Services 2003).



The integrated approach to information security

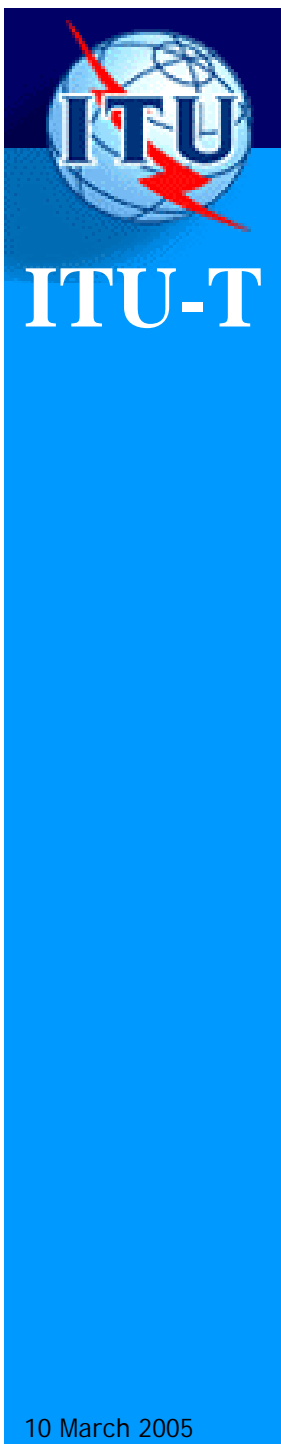
- o Creation of the new worldwide network for business communications.
 - Strict rules of behavior
 - Mandatory authorization
 - “Net-Police” / e-Interpol
 - Education and certification of users





Kaspersky Labs today

- Kaspersky Labs is the well-known world expert in the area of protection against computer viruses, malicious code, and spam.
- Kaspersky Labs has one of the best in the world technologies for detecting and removal of computer viruses and malicious code.
- Multinational company with representative offices all over the world (USA, UK, France, Germany, Poland, Netherlands, China, Japan, Ukraine, Kazakhstan, Belarus).
- Worldwide sales and partner's network.
- Integrated complete solution against all types of modern computer threats.
- Active participation in major industry associations and non-governmental organizations counteracting the dissemination of malicious code and spam.



Our mission

Our goal is to provide the most effective and secure protection against modern IT threats. We strive to be the fastest in detecting and blocking all threats.