

Спам как угроза информационной безопасности

Анна Власова

*Руководитель группы
спам-аналитиков*

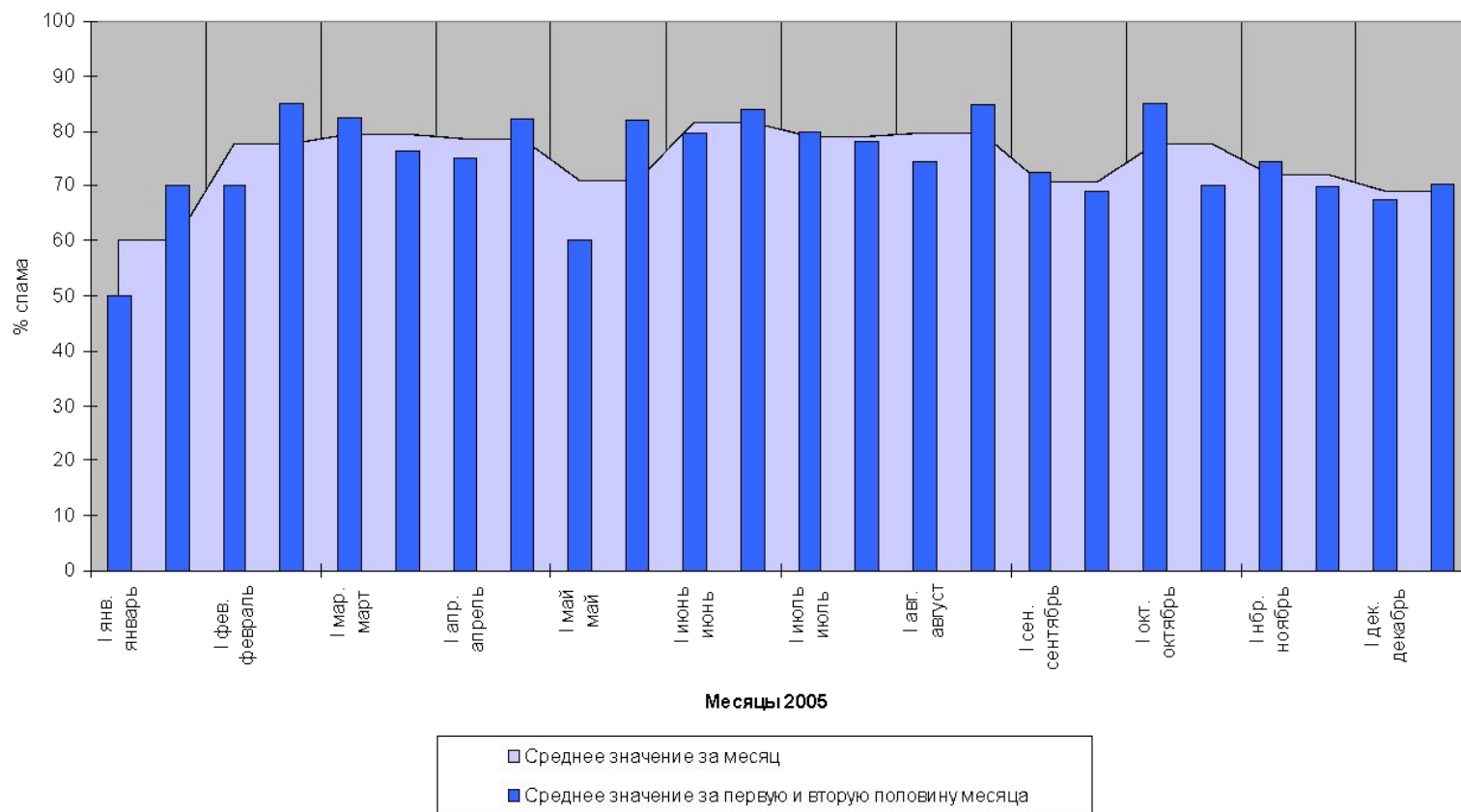
Anna.Vlasova@kaspersky.com

Угрожающие тенденции в развитии спама

- К 2005-му году доля спама стабилизировалась на уровне 70-80 %% от общего объема почтового трафика.
- Спам агрессивен и вызывает негативные эмоции.
- Спам стремительно криминализируется,
- Спам используется для распространения вредоносного ПО.

На каждые 2-3 обычных письма приходится 7-8 спамерских

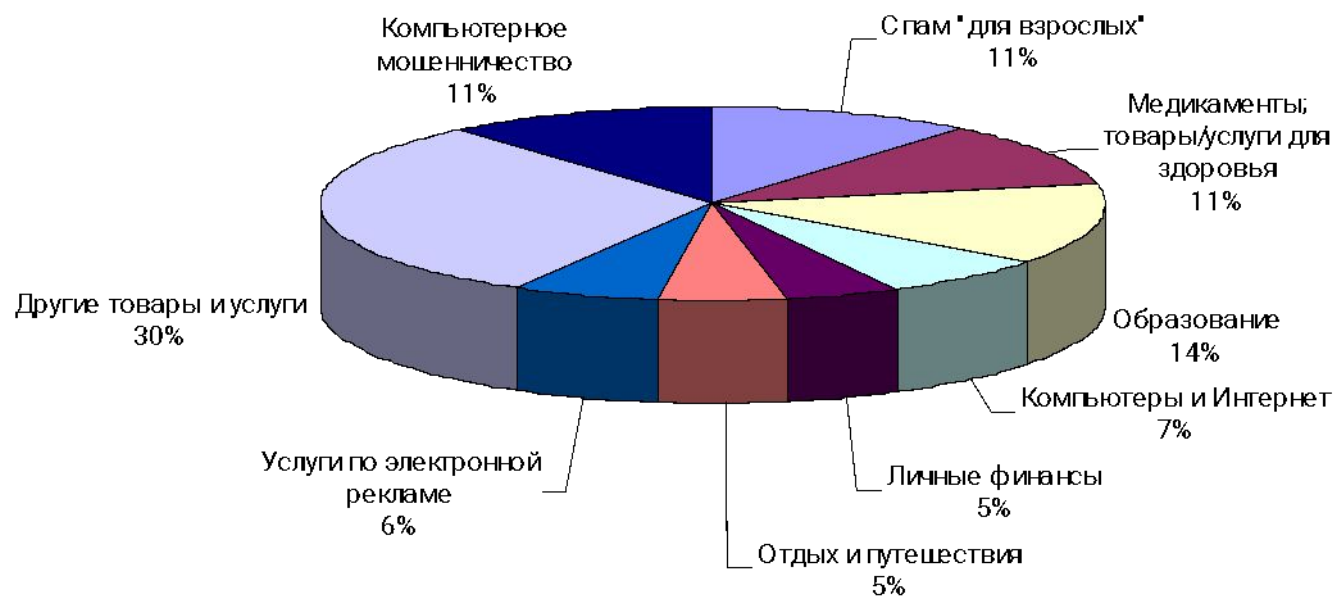
Количественное распределение спама в Рунете в 2005 году



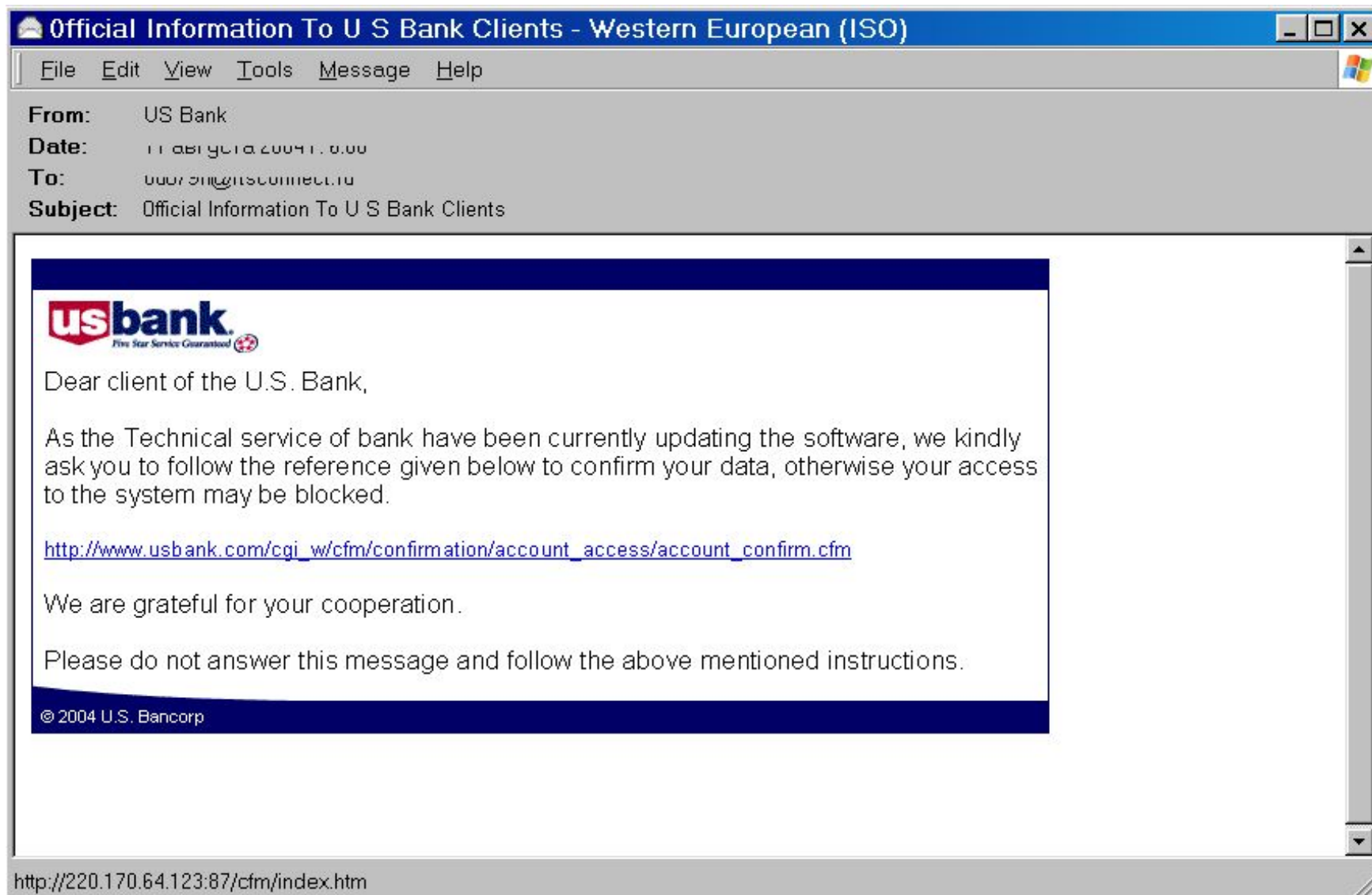
За последние два года спам быстро криминализируется

- высокая доля криминализованных спам-атак (6 – 20 %%);
- рост количества фишинг-атак (т.е. попыток украсть личную финансовую информацию);
- появление в спаме криминального бизнеса, не связанного с компьютерными технологиями;
- рост доли контрафактных и/или контрабандных товаров в спамерской товарной рекламе;
- использование спам-рассылок для «черного PR»;
- использование сетей зараженных персональных компьютеров (зомби-сетей) для рассылки спама.

Распределение тематик спама в Рунете в 2005 г.




Примеры криминализированного спама



The screenshot shows an email client window titled "Official Information To U S Bank Clients - Western European (ISO)". The email header includes:

- From:** US Bank
- Date:** 11.06.19.10.2004 11.00.00
- To:** 0007.011@riscconnect.ru
- Subject:** Official Information To U S Bank Clients

The email body contains the following text:


Dear client of the U.S. Bank,

As the Technical service of bank have been currently updating the software, we kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.


http://www.usbank.com/cgi_w/cfm/confirmation/account_access/account_confirm.cfm


We are grateful for your cooperation.

Please do not answer this message and follow the above mentioned instructions.

© 2004 U.S. Bancorp

The status bar at the bottom of the window shows the URL: <http://220.170.64.123:87/cfm/index.htm>

 We can upload trojan/virus to any computer - <http://prodownloader.com> - Western European (...)

File Edit View Tools Message Help 

From: webmaster@internationaloperation.com

Date: 4 марта 2006 г. 22:41

To: pop.comail.ru@mail.ru

Subject: We can upload trojan/virus to any computer - <http://prodownloader.com>

Dear Sir/Madam, Visit our site <http://prodownloader.com> We can infect millions of the users pc's with your trojan/virus for very low price 1000 infected pc's - 100\$ we have exploits, viruses, stolen credit cards & etc ! We can do botnet for you with your own zombied pc's for ddos or bank accounts grabbing ! FUCK SPAMHAUS !!!!! if they down our domain please use this ip adressess <http://85.255.112.132> <http://85.255.113.13> <http://195.95.218.100> msg-id: 909670

Putin and Bosh - TWO LOSERS! - Western European (ISO)

File Edit View Tools Message Help



Reply



Reply All



Forward



Print



Delete



Previous



Next



Addresses

From: subscription@kavkaz.uk.com
Date: 24 октября 2005 г. 21:34
To: [REDACTED]
Subject: Putin and Bosh - TWO LOSERS!

If you want to change your life,
If you want to live in freedom,
If you want to take off money from rich guys
And give it out to poor people,
It's time to big war!
Join to us!

Что же дальше?

- Криминализация может вызвать новый технологический скачок в развитии спама.
- В первую очередь спамеры будут бороться за скорость спам-рассылок, и обеспечение полиморфности спама.
- Возможны новые спамерские разработки в использовании графических файлов для отображения спама
- Развитие комплексной защиты электронной почты приведет к тому, что спамерам станет экономически выгодно использовать другие каналы распространения спама (например, мессенджеры)...

Электронная почта без защиты теряет функциональность. Антиспам - это такая же обязательная часть комплексной защиты, как и антивирус

Спасибо за внимание!