

Odbor sieťových služieb

V roku 2003 bol systém elektronickej pošty SAV realizovaný troma servermi. Všetky maily boli spracovávané serverom SAVBA a distribuované na príslušné servery. Hlavným problémom v tomto období boli vírusové infiltrácie, ktoré sa šírili elektronickou poštou. Antivírusová kontrola elektronickej pošty bola realizovaná prostredníctvom programu RAV, ktorého veľkým nedostatkom bola licenčná politika umožňujúca antivírusovú ochranu len pre určitý počet domén. Systém elektronickej pošty SAV obsluhoval v tomto čase väčší počet domén ako bolo zahrnuté v licencií programu RAV a preto mohlo dochádzať k šíreniu vírusových infiltrácií doručovaných na „neodvirené“ domény. Z tohto dôvodu bolo potrebné realizovať antivírusovú kontrolu iným spôsobom.

V prvej polovici roku 2004 bol inovovaný zálohovací systém a systémy náhradnej prevádzky v clusteri poštových serverov. Tým došlo k zvýšeniu operability systému, jeho spoľahlivosti a zabezpečila sa možnosť rýchlejšieho prechodu na záložnú prevádzku v prípade výpadku niektorého zo systémov. V druhej polovici roku bol systém elektronickej pošty doplnený o centrálny antivírusový server, ktorého hlavnou úlohou bolo kontrolovať všetky doručované maily na prítomnosť vírusov a zamedziť šíreniu vírusových infiltrácií v SAV prostredníctvom mailov. Antivírusový systém RAV bol nahradený programom antivírusovým systémom NOD32, ktorý bol licencovaný na počet používateľských schránok a nie na počet domén. NOD32 ako jeden z mála antivírusových produktov dosahoval veľmi dobré výsledky pri identifikácii vírusov a umožňoval nasadenie pod operačným systémom Linux. Správy, ktoré prešli antivírusovou kontrolou a obsahovali nežiaducu infiltráciu boli označené v predmete správy hlásením [NOD32 deleted] a identifikovaná nežiaduca príloha bola odstránená. Týmto sme zabezpečili aby všetky maily prijaté antivírusovým systémom boli doručované používateľom v SAV. Centrálny antivírusový server slúžil aj na kontrolu odchádzajúcej pošty na prítomnosť vírusov. Týmto sme sa snažili eliminovať potenciálne šírenie vírusov do siete internet. Úspešným zavedením antivírusovej kontroly však neskončil boj s nevyžiadanou poštou, pretože okrem vírusových epidémií dochádzalo k občasnému zahľteniu centrálného antivírusového systému, spôsobené veľkým počtom nevyžiadaných reklamných mailov (spamov). V čase epidémií bolo problematické prijímanie a odosielanie mailov zo SAV. K zahľteniu dochádzalo nielen na centrálnom antivírusovom systéme ale aj na serveri SAVBA, ktorý slúži na distribúciu mailov do používateľských schránok.

V roku 2005 bol systém doplnený o ďalšie servery a došlo k oddeleniu smerov prichádzajúcej a odchádzajúcej pošty. Bol sfunkčnený systém záložnej prevádzky pre centrálny antivírusový server. Server prichádzajúcej pošty je zálohovaný automaticky na základe DNS záznamov. Služby serveru odchádzajúcej pošty je možné v prípade poruchy presunúť na záložný systém, avšak tento zásah je potrebné realizovať manuálne. V snahe znížiť vyťaženie servera SAVBA ako aj ostatných serverov, ktoré spracovávajú maily, bola v roku 2005 zrealizovaná antispamová kontrola mailov. Všetky spracovávané maily sú na základe testov antispamového filtra bodované a závislosti od dosiahnutia bodového hodnotenie sú označované ako možná nevyžiadaná pošta. Táto skutočnosť je používateľovi oznamovaná doplnením textu “[SPAM]” do predmetu správy a je na používateľovi čo s týmito mailami spraví. Označované sú správy, ktoré dosiahli bodové hodnotenie väčšie ako 4.5 bodu. Na začiatku mesiaca apríl 2005 sme sa na základe sledovania funkčnosti antispamového filtra a odozvy používateľov rozhodli odstraňovať maily, ktoré dosiahli pri antispamovej kontrole bodové hodnotenie väčšie ako 15 bodov. V polovici mája sme túto hranicu znížili na 10 bodov. Vďaka týmto opatreniam sa nám podarilo odstrániť viac ako 25% spracovaných mailov. Postupným učením antispamového filtra a komunikáciou s používateľmi sa nám ku koncu roku 2005 podarilo zvýšiť úspešnosť odstraňovania nevyžiadaných mailov na viac ako 50%. Chybná identifikácia nevyžiadanej pošty predstavovala menej ako 0.001%, čo predstavovalo asi 5 chybné označených mailov z jedného milióna spracovaných mailov.

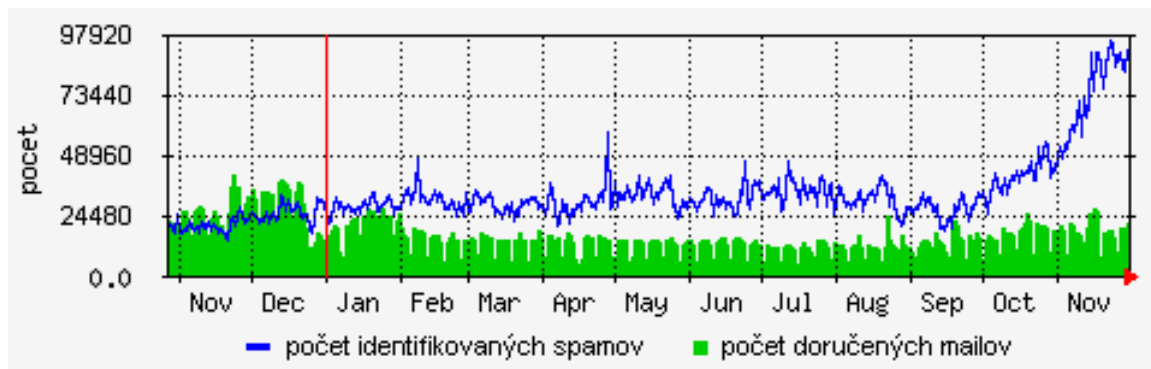
Antispamový systém sme naučili aby takéto maily nehodnotil ako nevyžiadaná pošta a tým sa pravdepodobnosť chybnjej identifikácie ešte znížila.

V oblasti videokonferenčných technológií sme sa zaoberali možnosťou poskytnutia videokonferenčných prenosov v snahe doniesť progresívne komunikačné technológie pre prenos zvuku i obrazu súčasne a zabezpečiť tak vedenie videokonferencií pre potreby SAV. V máji začala etapa prípravy malej videokonferenčnej miestnosti, ktorá skončila na konci roku 2005. Výsledkom bola funkčná videokonferenčná miestnosť pre 8 ľudí vybavená všetkou potrebnou technológiou pre zabezpečovanie videokonferencií.

V roku 2006 sme pokračovali v uplatňovaní nasadených postupov a postupným sledovaním a mesačným vyhodnocovaním nevyžiadanej pošty sa nám v máji roku 2006 podarilo znížiť hranicu odstraňovania nevyžiadanej pošty na 7 bodov a tým sme schopný odstrániť viac ako 75% spracovávaných mailov, ktoré by mali byť doručené do SAV, avšak boli vyhodnotené ako nevyžiadaná pošta.

V priebehu mesiaca október 2006 došlo k hromadnému šíreniu vírusu "Win32/Stration", ktorý spôsobil nárast mailovej komunikácie vo svete. Charakteristika vírusu sa veľmi rýchlo menila a preto dochádzalo v tomto období k vírusovým epidémiám.

Zo štatistík mailovej komunikácie na serveri prichádzajúcej pošty (obrázok č. 1), je možné vidieť že počet identifikovaných spamov (modrá čiara), počas mesiaca november prudko rastie a v porovnaní s predchádzajúcimi mesiacmi je tento nárast miestami aj dvojnásobný. Počet doručených mailov (zelená plocha), sa v mesiaci november mierne zvýšil. Tento stav je spôsobený neidentifikovaním niektorých spamov počas vírusových epidémií z dôvodu hromadného doručovania mailov z rôznych kútov sveta.



Obrázok č. 1 Denné priemery počtu mailov pre SAV z mesiaca november 2006

Z dôvodu zabezpečenia bezproblémového doručovania mailov bolo k 1. decembru 2006 upravené nastavenie antispamového filtra na prísnejšie hodnotenie spamov a bola znížená hranica odstraňovania nevyžiadanej pošty zo 7 bodov na 5 bodov.

Ku koncu roku 2006 bola vo VS SAV vybudovaná veľká videokonferenčná miestnosť, ktorá umožňuje realizáciu videokonferenčných prenosov pre 20 účastníkov.

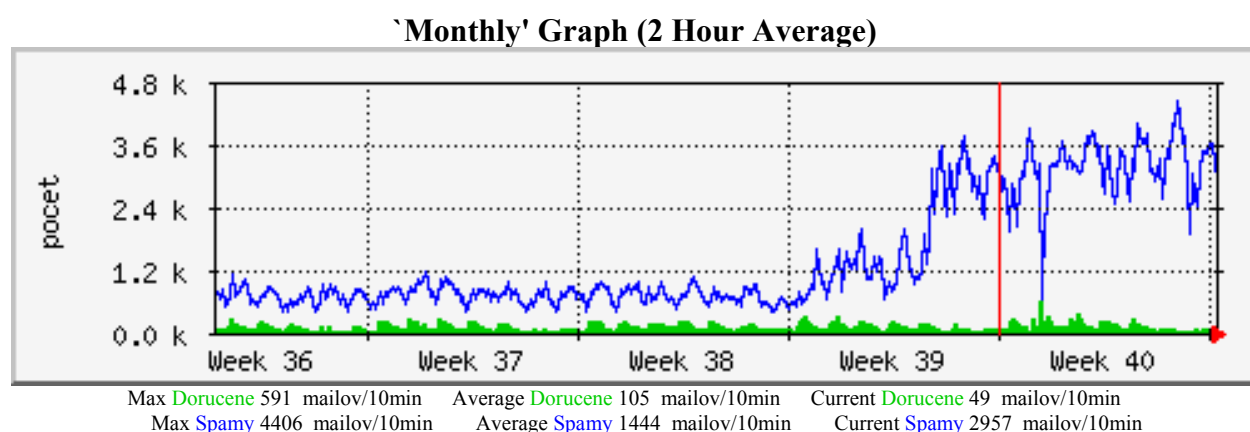
V roku 2007 sme postupným upravovaním antispamového filtra boli schopní odstrániť viac ako 90% všetkých spracovaných mailových správ. Tým však naše úsilie o zlepšenie poskytovaných služieb neskončilo. Od 1. mája 2007 bolo do testovacej prevádzky nasadené nové antivírusové riešenie na báze opensource riešenia ClamAV (<http://www.clamav.net/>) v snahe znížiť výdavky za antivírusový systém. Okrem tohto systému bol naďalej v prevádzke aj antivírusový systém NOD32, pomocou ktorého sme porovnávali schopnosť detekcie testovaného systému.

Antivírusovej kontrole predchádza antispamová kontrola realizovaná opensource riešením SpamAssassin, ktoré pri súčasnom nastavení dosahuje veľmi dobré výsledky.

Počas mesiaca máj bola úspešnosť detekcie vírusov pomocou riešenia ClamAV v porovnaní so systémom NOD32 viac ako 99,5%. Antivírusové riešenie pomocou ClamAV odhalilo okrem vírusových infiltrácií aj možné škodlivé obsahy, ktoré sa šírili vo forme html kódu, čo predstavuje oproti systému NOD32 veľkú výhodu.

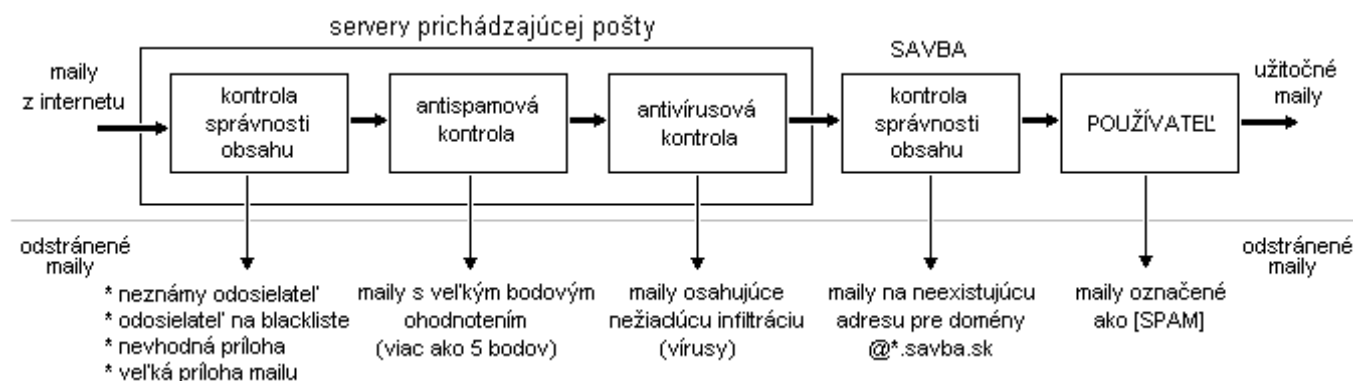
Začiatkom mesiaca september sa počet prijatých mailov pohyboval na hranici 100 mailov za jednu minútu. V mesiaci október tento počet stúpol viac ako trikrát (obrázok č. 2). Tento stav predstavoval kritickú hodnotu pri doručovaní mailov. V prípade, že tento počet mailov prekročí hranicu 400 mailov za minútu dochádza k zahlteniu mailového serveru a spomalovaniu doručovania mailov. V prípade, že tento stav pretrváva dlhšiu dobu môže dôjsť k preťaženiu systému a je potrebný zásah administrátora, ktorý tento stav musí vyriešiť iným spôsobom (napr. dočasným zablokovaním prijímania mailov, aby bolo možné doručiť čakajúce maily).

V prípade, že by bol tento stav spôsobený rozposielaním nevyžiadaných mailov z jednej IP adresy, bol vytvorený systém automatického kontrolovania a vyhodnocovania potenciálnych hrozieb. V prípade prekročenia stanovenej hranice počtu pripojení na mailový server, bol prístup k serveru z tejto IP adresy zablokovaný. Jednalo sa však o rozposielanie z viacerých adries a nie viac ako 500 pripojení z jednej a preto bol problém zložitejší.



Obrázok č. 2 Dvojhodinové priemery počtu mailov pre SAV z mesiaca október 2007

Maily, ktoré prejdú antivírusovou a antispamovou kontrolou sú preposielané na hlavný poštový server, ktorý ich ďalej distribuuje do používateľských schránok, odkiaľ si ich používatelia vyzdvihnú pomocou klientov elektronickej pošty. V prípade veľkého množstva požiadaviek zo strany používateľov, dochádzalo k preťaženiu serverov s používateľskými dátami a tým aj spomalenie komunikácie s poštovými servermi.



Obrázok č. 3 Proces spracovávaní mailových správ pri doručovaní používateľom

Vo všeobecnosti

Aj naďalej je však potrebné sledovať aktivity súvisiace s doručovaním nevyžiadanej pošty aby sme boli v prípade zistenia nadmernej komunikácie schopní včas reagovať a vyriešiť prípadný problém. Z tohto dôvodu sú každých 10 minút vyhodnocované počty mailov spracovávaných mailovými servermi. Tieto hodnoty sú vynášané do grafov umiestnených na webovských stránkach. Tým je umožnená jednoduchšia identifikácia chybových stavov v prípade problémov s doručovaním pošty.

Prevádzkovaním dvoch videokonferenčných miestností sme poskytovali možnosť využiť ich technológiu pre videokonferencie vedené z pôdy SAV. Túto možnosť využilo niekoľko ústavov i Úrad SAV. Prebehlo i niekoľko kurzov, ktoré boli prenášané cez internet a mohli ich sledovať záujemcovia z radov pracovníkov SAV priamo na svojich pracoviskách.

Počas roku 2007 sme zabezpečili vybudovanie videokonferenčného centra v Kongresovom centre SAV v Smoleniciach pričom sme využili ročné skúsenosti z prevádzkovania videokonferenčných miestností vo VS SAV.

Podrobný rozpis aktivít za rok 2007 v tejto oblasti je v tab. č. 1

dátum	aktivita
5.1.2007 -	Videopiatok vo VS SAV
12.1.2007 -	Videopiatok vo VS SAV
16.1.2007 -	Prednáška o videokonferencii
19.1.2007 -	Videopiatok vo VS SAV
23.-25.1.2007 -	Videokonferencia pre Archeologický ústav SAV
8.2.2007 -	Prenos z otvorenia videokonf. miestnosti v Košiciach
9.2.2007 -	Videopiatok vo VS s pracovníkmi nového uzla v Hurbanove
12.2.2007 -	Testovací prenos zo Smoleníc pre 1. odd.
13.-14.2.2007 -	Videopiatok vo VS SAV
16.2.2007 -	Prenos z evalvačného seminára 1. odd. SAV zo Smoleníc
20.2.2007 -	Prenos zo slávnostného otvorenia uzla SANETu v Geografickom ústave Hurbanovo
16.3.2007 -	Výmena pracovníka na pozícii Obsluha videokonferencie. Pani Eva Kohútová odišla, prišiel pán Viktor Valentíny
11,12,13.9.2007 -	prenos z konferencie poriadanej Ústavom experimentálnej endokrinológie (SjF STU) Školenie PZ20
19.9.2007 -	KiT;

28.9.2007 -	prenos zo školenia PZ19;
1.10.2007 –	videorozhovor s kandidátom na post riaditeľa, s p. Novockým;
4.10.2007 –	videorozhovor -pohovor s kandidátom na funkciu riaditeľa ústavu.
15.11.2007 -	prenos z konferencie poriadanej Ústavom hudobnej vedy SAV
28.11.2007 -	prezentácia systému ELVYS formou videokonferencie
11.12.2007 -	Testovanie kvality spojenia videokonferencie pre potreby Chemického
14.12.2007 –	ústavu SAV

Prevádzkované služby

V súčasnosti odbor sieťových služieb prevádzkuje nasledovné služby:

- Služby pre prístup k používateľským dátam prostredníctvom protokolov POP3-SSL, IMAP-SSL, SSH alebo s použitím prístupu cez Webmail, ktoré využíva cca. 2700 používateľov na serveroch elektronickej pošty pre SAV umiestnených vo VS SAV.
- Filtrovanie nevyžiadanej pošty pomocou antivírusovej a antispamovej kontroly mailov
- Ukladanie logov zo systémov pre prípadnú analýzu chybových stavov
- Službu DNS pre prevod internetových mien na IP adresy a naopak. V súčasnosti spravujeme záznamy pre 56 domén, z toho sme priamo zodpovední za 33 domén (master DNS) a poskytujeme záložnú službu pre 23 domén (slave DNS)
- **Poskytovanie** služieb v oblasti videokonferenčných technológií

V súčasnosti servery antivírusovej a antispamovej kontroly spracovávajú viac ako 10 miliónov mailov mesačne a sme schopní identifikovať a odstrániť viac ako 95% správ, ktoré sú vyhodnotené ako nevyžiadaná pošta. Percento chybného označenia pošty je veľmi malé a nepredstavuje ani 0.001%. V porovnaní s predchádzajúcimi rokmi sa počet spracovávaných mailov zvýšil a dá sa predpokladať, že tento trend bude pokračovať aj v ďalších rokoch a to hlavne z dôvodu neustále sa zvyšujúcej priepustnosti siete internet a zväčšujúcim sa počtom počítačov do nej pripojených.

Antispamové riešenie sa javí ako veľmi dobré z hľadiska identifikácie nevyžiadanej pošty, avšak v prípade nového druhu spamovej epidémie systém nereaguje okamžite ale potrebuje určitú dobu na naučenie sa identifikovať daný druh spamov.

Antivírusová kontrola je realizovaná až po odfiltrovaní spamov a preto je percento identifikácie vírusov veľmi nízke a dlhodobo neprekročilo hranicu 1%. V prípade výpadku antispamového filtra je potrebné zamedziť šírenie vírusov prostredníctvom mailov a preto je potrebná realizácia antivírusového filtra.

	2005	2006	2007
Január	1 403 490	1 811 910	5 338 460
Február	1 223 330	1 670 123	5 541 577
Marec	1 136 855	1 909 124	5 587 380
Apríl	1 208 196	1 939 396	5 504 233
Máj	1 546 729	2 192 103	4 812 377
Jún	1 455 399	2 298 812	5 291 679
Júl	1 842 176	2 253 128	5 440 522
August	1 271 094	2 204 757	5 440 522
September	1 154 363	1 913 766	7 037 072
Október	1 307 467	2 616 071	17 766 655
November	1 276 702	3 861 524	15 912 120
December	1 524 876	5 024 990	14 826 211

Štatistiky počtov mailových správ za roky 2005-2007

