

# История антивирусного проекта ДиалогНауки

**Антимонов С.Г.**

**Председатель совета директоров  
ЗАО «ДиалогНаука»**



# **ЗАО «ДиалогНаука»**

**Создано в январе 1992 г. на базе Научного центра СП «Диалог» при Вычислительном центре РАН**

**Научный центр был образован в декабре 1989 г.**

**Учредители:**

- СП «Диалог» и**
- Вычислительный центр РАН**

**Антивирусные программы:**

**1990 - сканер Aidstest Лозинского Д.Н.**

**1991 - ревизор дисков ADinf Мостового Д.Ю.**

**1994 - семейство программ Doctor Web Данилова И.А.**

**2004 - семейство программ компании Sybari**

# СП «Диалог»

- 1987, первое российско-американское СП в области вычислительной техники и программного обеспечения
- эксклюзивная дистрибуция продуктов фирмы Microsoft в течение первых 2 лет
- 1990, визит Билла Гейтса в Москву в связи с выходом версии MS-DOS 4.01, локализованной на русский язык
- локализация на русский язык других продуктов как компании Microsoft, так и других компаний
- разработка отечественных пакетов программ

# Вычислительный центр РАН

- 1957, расчеты для 1-го искусственного спутника Земли
- 1967, БЭСМ-6, компиляторы для языка АЛГОЛ-60 и др.
- 1983, феномен «ядерной зимы»,  
академик Моисеев Никита Николаевич
- 1985, программы Лексикон и Мастер  
Евгения Веселова
- 1989, игра Тетрис  
Вадика Герасимова и Алексея Пажитнова

# **Антивирус Aidstest**

- 1988, 17 ноября Лозинский Д.Н. создал 1-ю версию**
- 1990, 1 октября мы заключили контракт с Лозинским Д.Н.**
- 1990, 10 октября на Софтуле продавали 44-ю версию**
- 1994, октябрь, 5-летие ADinf-a и 1001-я версия Aidstest**
- 1998, 17 ноября исполнилось 10 лет Aidstest-у**

**Лозинский Д.Н. по-прежнему активно участвует в различных разработках программ семейства Dr.Web**

# **Антивирусы ADinf & Cure Module**

- 1989, октябрь, Мостовой Д.Ю. создал 1-ю версию Dinf**
- 1990, 14-17 ноября на конференции в Киеве программа Dinf была признана лучшей в своем классе ревизоров**
- 1991, апрель, контракт с Мостовым Д.Ю. по ADinf-y**
- 1993, январь, контракт с Ладыгиным В.С., Зуевым Д.Г. и Мостовым Д.Ю. по программе ADinf Cure Module. В то время 97% всех зараженных файлов м.б. восстановить!**
- 2004, июнь, вышла версия 3.02 программы ADinf32**

# **Антивирус Doctor Web**

- 1991, SpIDer Web, книга Безрукова Н.Н.**
- 1993, европейский конкурс 1&1 перед CeBIT-1993**
- 1994, Doctor Web для DOS**
- 1996, первое участие в тестах журнала Virus Bulletin (VB)**
- 1999, Doctor Web для Windows**
- 2002, наилучшие результаты в тестах Virus Bulletin (февраль) и VTC Гамбургского университета (март)**

# **Антивирусы от компании Sybari**

**Компания Sybari создана в 1995 г. и первые ее продукты:**

- в 1996 г. антивирус Antigen 3 для Lotus Notes и**
- в 1997 г. антивирус Antigen 5 для Microsoft Exchange 5.0**

**И сейчас ее основные продукты -- это антивирусные решения Antigen для MS Exchange & Lotus Domino.**

**Продукты Antigen защищают в 50 странах мира более 9 млн. рабочих мест у 9 тыс. клиентов.**



# **Мировые потери от вирусов и спама**

**Потери мирового крупного бизнеса от вирусов:**

**1999 - 12,1 млрд. долл.**

**2000 - 17,1 млрд. долл. (около 50% - LoveLetter)**

**2001 - 13,2 млрд. долл.**

**2002 - 14,5 млрд. долл.**

**2003 - 55,0 млрд. долл. (более 70% - SoBig, Blaster)**

**2004 - 68,7 млрд. долл. только от MyDoom**

**Потери в мире от спама:**

**2001 - 10 млрд. евро**

**2002 - 15 млрд. евро**

**2003 - 20 млрд. евро**

# **Основные вирусописатели – школьники и студенты**

**1997 - "WM.Cap", учащийся 15 лет из Венесуэлы**

**1998 - "Чернобыль", студент из Тайваня**

**2000 - "Love Letter", студент из Филиппин**

**2001 - "Anna Kournikova", 20-летний голландец**

**2002 - "Goner", 5 учеников 8-11 классов из Израиля**

**2003 - "Blaster" (одна из версий), американец 18 лет**

**2004 – "Sasser" и семейство "Netsky", немец 18 лет**

# **Действия компании Microsoft, направленные на борьбу с вирусописателями**

**Ноябрь 2003 - \$5m в фонд борьбы с вирусописателями. Было выделено 3 \* 250 тыс. долл. – на поиски авторов вирусов Blaster.A, SoBig.F и MyDoom.B. Компания SCO выделила 250 тыс. долл. за «голову» автора MyDoom.A.**

**Май 2004, арестовали создателя вирусов Sasser и Netsky.**

**В 2003 г. была куплена румынская антивирусная фирма GeCAD и на днях MS объявил, что будет делать свой АВ.**

# **ICSA Labs о распространенности вирусов в 2003 (Computer Virus 9<sup>th</sup> Annual Prevalence Survey 2003)**

**300 респондентов -- организации государственного, коммерческого и промышленного секторов.**

**Средняя компьютерная мощность: более 500 компьютеров, 2 и более локальных сетей, 2 и более точек удаленного доступа к корпоративной сети.**

**Все респонденты отметили, что проблем с компьютерными вирусами становится все больше.**

# **Количество обнаруженных вирусов в месяц в среднем на 1000 компьютеров (ICSA Labs)**

<b>Год</b>	<b>Количество вирусов</b>
<b>1996</b>	<b>10</b>
<b>1997</b>	<b>21</b>
<b>1998</b>	<b>32</b>
<b>1999</b>	<b>80</b>
<b>2000</b>	<b>91</b>
<b>2001</b>	<b>103</b>
<b>2002</b>	<b>105</b>
<b>2003</b>	<b>108</b>

# Каналы проникновения вирусов в компьютеры (ICSA Labs 2003 survey)

Источники вирусов	1996	1997	1998	1999	2000	2001	2002	2003
Вложения в электронные письма	9%	26%	32%	56%	87%	83%	86%	88%
Файлы, загружаемые из Интернета	10%	16%	9%	11%	1%	13%	11%	16%
Просмотр веб-сайтов	0%	5%	2%	3%	0%	7%	4%	4%
"Не знаю"	15%	7%	5%	9%	2%	1%	1%	3%
Другие пути	0%	5%	1%	1%	1%	2%	3%	11%
Дистрибутив ПО	0%	3%	3%	0%	1%	2%	0%	0%
Дискеты	71%	84%	64%	27%	7%	1%	0%	0%

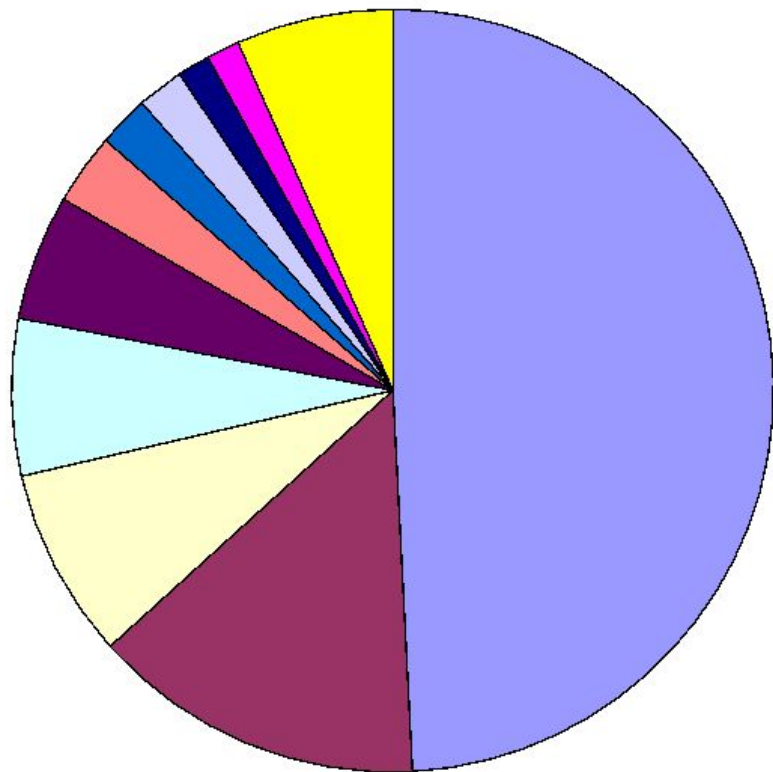
# **Решения Dr.Web для почтовых серверов, работающих под управлением Unix-систем**

**Демон Dr.Web для Unix-систем Linux, FreeBSD, OpenBSD и Solaris (x86) может быть использован практически в любых комплексах обработки данных в качестве подключаемого внешнего антивирусного фильтра.**

**Есть готовые антивирусные фильтры для почтовых серверов Sendmail, QMail, Postfix, Exim, CommuniGatePro, Courier-MTA, Zmailer и Mobicо MIO.**

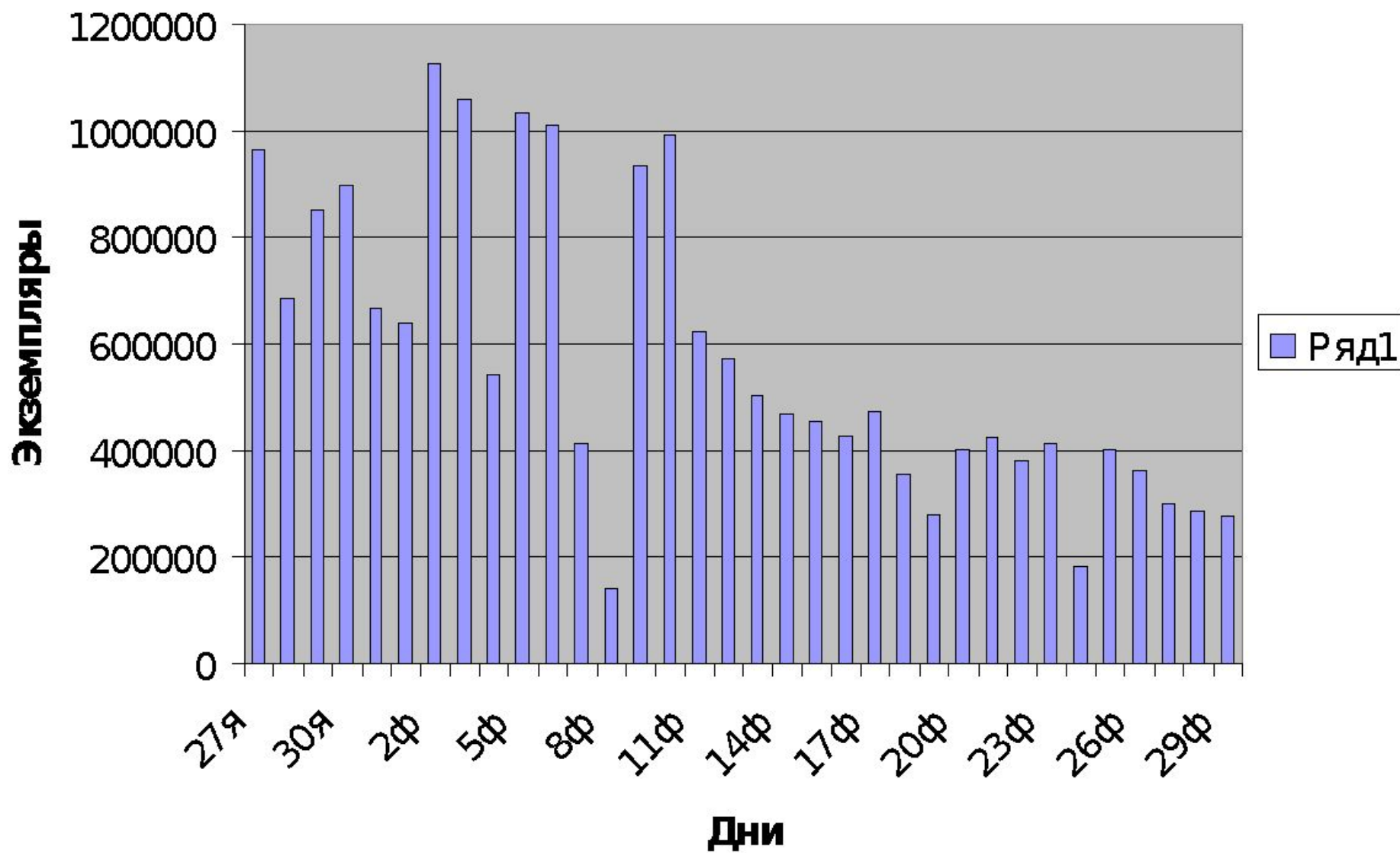
**Используются на почтовых серверах Mail.ru, Яндекс, Зенон, РосБизнесКонсалтинг, HighWay, Петерлинк и др.**

**В январе-феврале 2004 г. более 40 млн. экз. вирусов Dr.Web обезвредил в России на крупнейших почтовых серверах Mail.ru, Яндекс, Зенон, РосБизнесКонсалтинг, HighWay, Петерлинк и др.**

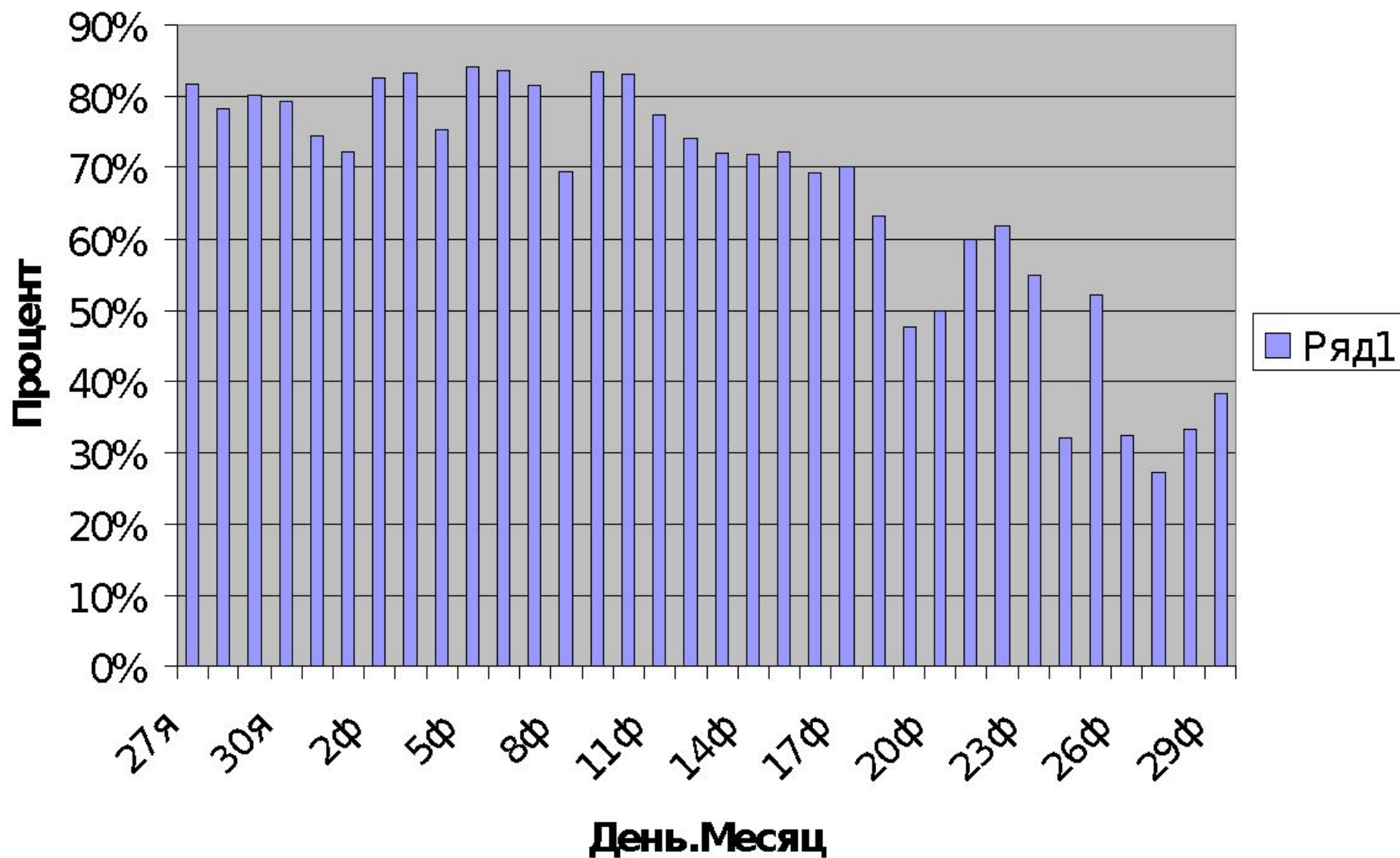




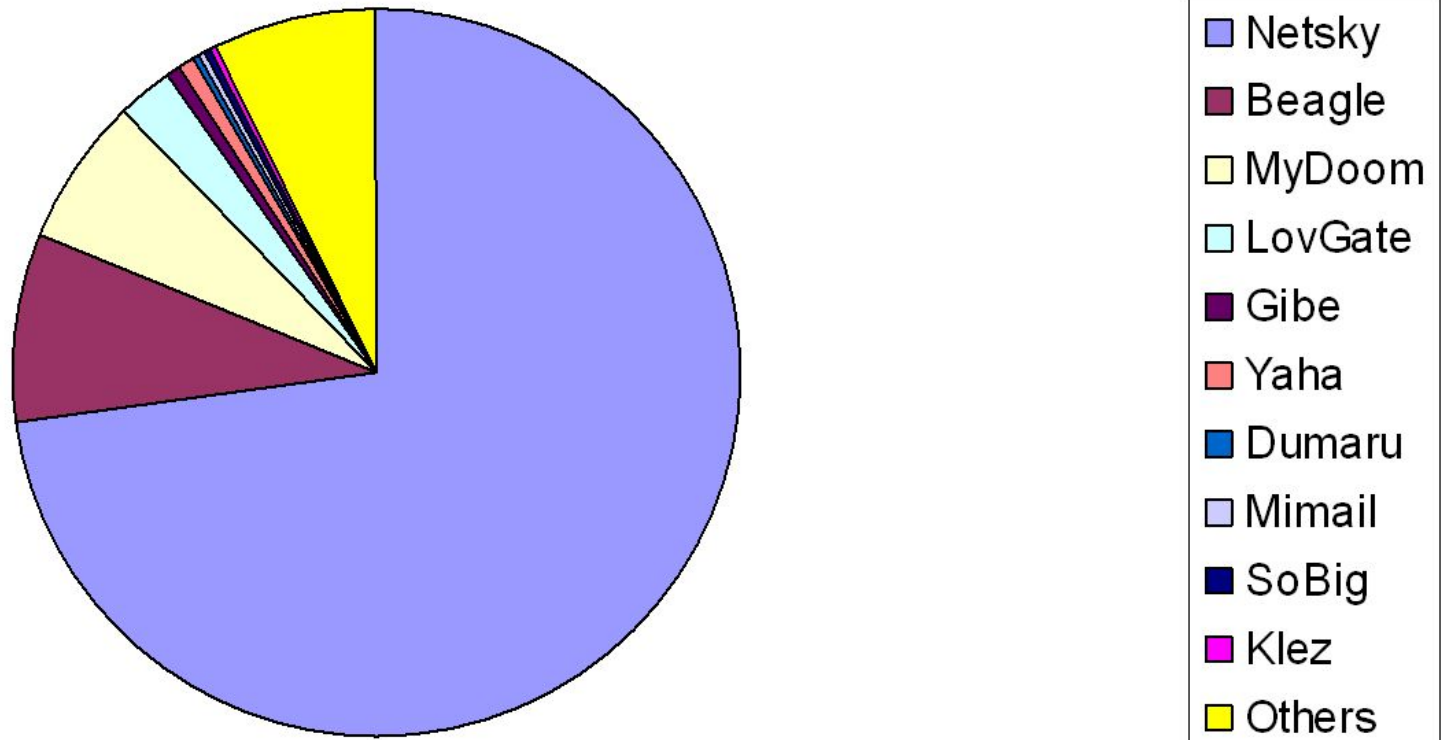
# Win32.HLMM.MyDoom.32768



# Процент MyDoom.32768 в общем объеме



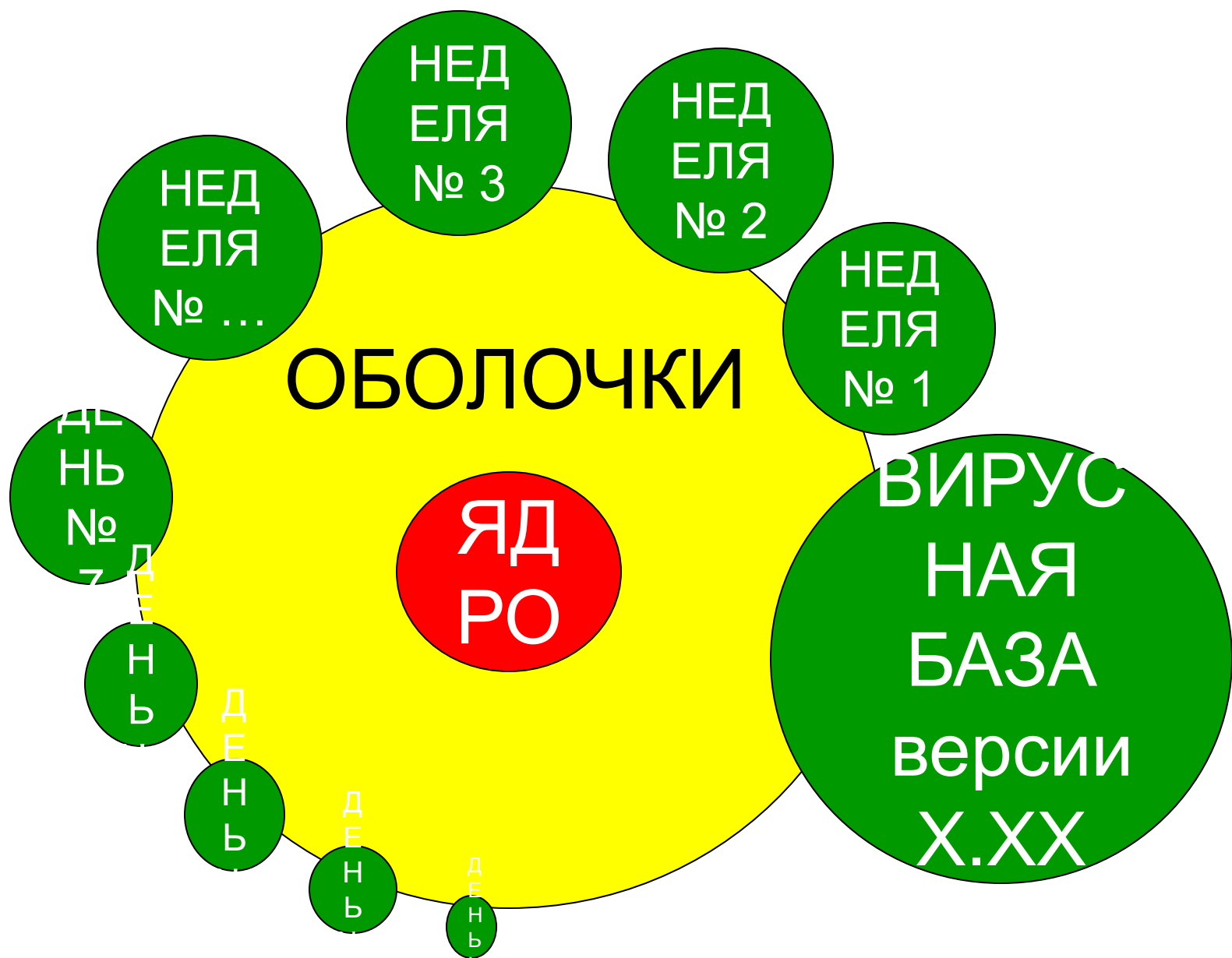
**120 млн. экз. -- в "Апреле-Мае 2004"  
(с учетом данных от серверов Telia)**



# **Антивирусные продукты Antigen от компании Sybari**

- Antigen 7.5 для серверов почты Microsoft Exchange**
- Antigen 7.5 для шлюзов SMTP Gateways**
- Antigen 7.0 для серверов почты Lotus Domino**
- Antigen 7.5 для серверов Microsoft SharePoint**
- Antigen 7.5 для серверов Instant Messaging**

# Модульный принцип антивируса



# **Оболочки антивирусных программ**

**Windows 95/98/Me/NT/2000/XP**

**Linux, FreeBSD, OpenBSD, NetBSD, Solaris x86, MCBC**

- почтовые серверы Sendmail, Qmail, PostFix, Exim, Zmailer, CommuniGate Pro, Courier-MTA и**
- файловый сервер Samba**

**Windows NT/2000/XP, MS Exchange, Lotus Notes, NetWare**

**DOS, Windows 3.1x, OS/2**

**Ядро (DLL) антивируса встраивается также и в другие  
прикладные программы**

# **Лицензирование ядра Dr.Web другим производителям**

**1999 -- система документооборота «Сапиенс» фирмы НПО «Машиностроения» (Россия), антивирусная проверка файлов перед их записью в базу данных**

**2000 -- антивирусная программа iDuba.net фирмы Kingsoft (Китай), использует два ядра («движка»)**

**2001 -- программа Nero записи файлов на CD-R фирмы Ahead (Германия), проверка перед «прожиганием»**

**2001 -- антивирус StopSign фирмы eAcceleration (США)**

**2002 -- антивирус Virus Chaser фирмы NWI (Южная Корея), продается в Южной Корее и в Японии с 2002 года**





# **Тестирование антивирусов в Virus Test Center при Гамбургском университете, март 2002 г.**

**Тестирование старых версий антивирусов.**

**Совершенно новые вирусы обнаруживались:**

- как модификации старых вирусов,**
- как представители уже известных семейств вирусов,**
- с помощью эвристических алгоритмов.**

**В этих тестах, в которых принимали участие лучшие антивирусы со всего мира, Doctor Web был отмечен как показавший наилучшие результаты.**

# **Программы Doctor Web и ADinf сертифицированы Министерством обороны РФ**

**Программы прошли испытания в части соответствия реальных и декларируемых функциональных возможностей, отсутствия недекларированных возможностей (программных закладок).**



**Это был первый случай получения антивирусными программами такого сертификата соответствия**

# **Интеграция Doctor Web в компьютеризированные системы**

**С 1995 - ГАС “Выборы”, Центробанк**

**С 1996 - ГУИР ФАПСИ, Сбербанк**

**С 1997 - Минфин, ФСНП**

**С 1998 - Минобороны, Минобразования**

**С 1999 - Минэкономики, Минпромнауки**

**С 2000 - Аппараты Госдумы и Совета Федерации**

**С 2001 - Министерство по налогам и сборам**

**С 2002 - Пенсионный фонд**

**С 2003 - Вторая очередь ГАС «Выборы»**

# Бесплатная лицензия для учебных заведений Министерства образования РФ



Шестой год подряд мы даем бесплатную лицензию Министерству образования России для использования антивирусов Doctor Web и ADinf в государственных учебных заведениях.

Программы используются в десятках тысяч учебных заведений России.

Распространяются программы через сервер Министерства образования РФ

# Меморандум АДЭ

**Меморандум о противодействии распространению вредоносных программ (вирусов) и несанкционированных рекламных рассылок (спама) разработан общественно-государственным объединением “Ассоциация Документальной Электросвязи” (АДЭ) в соответствии с поручением Министра Российской Федерации по связи и информатизации.**

# **Участники разработки и обсуждения Меморандума**

**В разработке и обсуждении Меморандума участвовали представители государственных организаций и коммерческих компаний -- АДЭ, Ашманов и Партнеры, ДиалогНаука, Зенон Н.С.П., Инфосистемы Джет, ИСА РАН, Лаборатория Касперского, Майкрософт, Минсвязи РФ, МТУ-Интел, РосНИИРОС, Ростелеком, РТКомм.РУ, ТрансТелеКом, Совинтел, Яндекс, Cisco Systems, Mail.ru, Rambler и др.**

**Полный текст Меморандума представлен на сайте АДЭ.**

# **План работ АДЭ на 2004 по выполнению задач, поставленных в Меморандуме**

**I. Нормативно-правовая деятельность.**

**II. Разработка стандартов.**

**III. Просвещение.**

# **I. Нормативно-правовая деятельность**

**НИР «Сравнение законодательств России, США и Европейского союза в области информационной безопасности».**

**Разработка предложений по законодательным мерам противодействия вирусным угрозам и спаму.**



# **II. Разработка стандартов**

**Нормативный акт «Компьютерные вирусы. Основные термины и определения».**

**Профили защиты «Средства антивирусной защиты».**

**Профили защиты «Средства борьбы с несанкционированной рассылкой».**

# III. Просвещение

**Разработка учебных программ и проведение учебных курсов.**

**Разработка учебного пособия «Защита информационных ресурсов от вирусных угроз и спама».**

**Создание раздела сайта АДЭ по противодействию распространению вредоносных программ и спама.**

---

**The US Computer Emergency Readiness Team:  
[www.US-CERT.gov](http://www.US-CERT.gov) -- новости и советы в области  
информационной безопасности ПК**

# Юридические задачи

**19 августа 2003 фирма Symantec за 62,5 млн. долл. купила у фирмы Hilgraeve патент США за № 5,319,776 от 1997г.**

**В 1997 Hilgraeve подала в суд на Symantec и McAfee (NAI).**

**NAI, Trend Micro и IBM уже урегулировали этот вопрос.**

**Дела Computer Associates, Aladdin Knowledge Systems и Clearswift до сих пор в суде. «Дожимать» будет Symantec.**

**The patent describes hardware and software implementations of scanning data intransit between two 'mediums', such as 'between two computer[s] communicating over a telecommunications link or network'.**

# Спасибо за внимание!



**Адрес: 119991, Москва, ул. Вавилова, д. 40, офис 103**

**Тел.: (+7 095) 137 0150, 135 6253**

**Тел./факс: (+7 095) 938 2970, 938 2855**

**Интернет-представительство: [www.DialogNauka.ru](http://www.DialogNauka.ru)**

**Электронная почта: [Antivir@DialogNauka.ru](mailto:Antivir@DialogNauka.ru)**