

# Инструменты управления Интернетом

# История, организации.

1979 — Управляющий совет по определению структуры Интернета, основана DARPA для контроля развития сети.

1984 — переименована в Совет архитектуры Интернета (он же Internet Advisory Board, Internet Architecture Board)

1986 — переименована в Совет развития Интернета.

1986 — Оперативная группа по разработке стандартов Интернета, создана правительством США для развития и поддержки Интернет-стандартов.

Йон Постел (Jon Postel) предложил передать распределение адресов (для различных протоколов Интернета) в ведение подразделения компьютерных сетей Института информационных технологий Университета Южной Калифорнии, что было сделано с одобрения и с учётом контракта с Министерством Обороны США. Эта роль позже перешла к Организации по учёту распределённых адресов в Интернете (IANA) и включила также менеджмент корневых серверов системы доменных имён. Йон также работал редактором Службы запроса комментариев.

Распределение IP адресов делегировано четырём организациям Региональных регистров Интернета:

- американский (ARIN) - для Северной Америки
- европейский (RIPE NCC) - для Европы, Ближнего Востока и Центральной Азии
- азиатско-тихоокеанского (APNIC) - для Азиатско-тихоокеанского региона
- латиноамериканско-карибский (LACNIC) - для стран Латинской Америки и Карибского бассейна
- С 2004 года к ним добавился африканский для стран Африки.

1998 г - в сентябре после смерти Постела, функции IANA были переданы Корпорации Интернета по учёту распределённых имён и номеров (ICANN), в соответствии с Постановлением Правительства США и с контрактом с Министерством Торговли США. Первоначально лишь два члена Совета управляющих этой организации выбирались Мировым сообществом Интернета, что, однако, было изменено в 2002 году на совещании в Гане (Аккра).

Миссия Мирового сообщества Интернета (ISOC), основанного в 1992 году была сформулирована тогда же и гласит, что организация создаётся для «гарантии свободного развития и использования Интернета для блага всего человечества». Её членами могут стать любые физические и юридические лица, в числе последних Государственные органы и Университеты. Совет по архитектуре Интернета (IAB) позже стал частью Мирового сообщества Интернета вместе с Оперативной группой по разработке стандартов Интернета (IETF). Последняя на сегодняшний день регулируется Управляющей группой по разработке стандартов Интернета (IESF), в то время как долговременные исследования переданы в ведение Оперативной группы по Интернет исследованиям регулируемой Управляющей группой по Интернет исследованиям.

# Организации:

*IETF — the Internet Engineering Task Force*

*Number Resource Organization*

*RIRs — Regional Internet Registries*

*ISOC — the Internet Society*

*Организации ООН по управлению Интернетом*

*Internet Governance Forum*

*World Summit on the Information Society*

*Working Group on Internet Governance*

# ИНТЕРНЕТ СЕГОДНЯ:

---

- ✘ Основа для творчества, общения, реализации прогрессивных идей
- ✘ Информационный контур системы управления по международным стандартам
- ✘ Удаленное администрирование и контроль
- ✘ Доступ к информации
- ✘ Автоматизация торговли
- ✘ Прогрессивная реклама
- ✘ Досуг: развлечения, медиа, игры и др.



# Правовое регулирование ПО складывающихся в Интернете

---

- ✗ - международное;
- ✗ - региональное (в рамках Европейского союза и СНГ);
- ✗ - национальное.

*Унификация норм проводится как в рамках ЕС, так и на международном уровне в рамках ООН (институт унификации частного права УНИДРУА), Всемирной Организации Интеллектуальной собственности (ВОИС); Международной торговой палатой (МТП); Европейской экономической комиссией ООН; Центром ООН содействия торговле и электронному бизнесу.*

*Ежегодно Internet Corporation for Assigned Names (ICANN) проводятся международные конференции по проблеме унификации норм, направленных на регулирование Интернет.*

*комиссия ООН по праву международной торговли (ЮНСИТРАЛ). В числе прочих актов названного органа необходимо выделить:*

- Типовой закон ЮНСИТРАЛ «Об электронной коммерции» 1996г. (с дополнительной статьей 5 bis, принятой в 1998г.);*
- Типовой закон ЮНСИТРАЛ «Об электронных подписях» 2001г.*

*Советом Европы приняты следующие акты:*

- Конвенция «О защите физических лиц в отношении автоматической обработки персональных данных» от 28 января 1981г. (Страсбург);*
- Дополнительный протокол к Конвенции о защите физических лиц в отношении автоматической обработки персональных данных, касающийся надзорных органов и трансграничных потоков данных от 8 ноября 2001г. (Страсбург);*
- Конвенция об информационном и правовом сотрудничестве, касающемся «услуг информационного общества» от 4 октября 2001 г.;*
- Конвенция Совета Европы по киберпреступности от 23 декабря 2001г.*

✘ Европейское право сети Интернет включает в себя множество директив и резолюций:

---

- ✘ - Директива 97/7/ЕС Европейского парламента и Совета от 20 мая 1997 г. о защите потребителей в отношении дистанционных договоров (дистанционная продажа);
- ✘ - Директива 97/66/ЕС Европейского парламента и Совета от 15 декабря 1997 г., касающаяся обработки персональных данных и охраны тайны частной жизни в телекоммуникационном сектор;
- ✘ - Директива Европейского парламента и Совета 1999/93/ЕС от 13 декабря 1999 г. о правовых основах Сообщества для электронных подписей;
- ✘ - Директива 2000/31/ЕС Европейского парламента и Совета от 8 июня 2000 г. о некоторых правовых аспектах услуг информационного общества, в том числе электронной коммерции, на внутреннем рынке (Директива об электронной коммерции);
- ✘ - Директива 2000/46/ЕС Европейского парламента и Совета от 18 сентября 2000 г. о занятии, осуществлении и надзоре за предпринимательской деятельностью учреждений в сфере электронных денег;
- ✘ - Директива 2002/58/ЕС Европейского парламента и Совета от 12 июля 2002 г., касающаяся обработки персональных данных и охраны тайны частной жизни в секторе электронных коммуникаций;
- ✘ - Резолюция Европейского парламента о безопасном использовании Интернет и новых on-line<sup>[1]</sup> (он-лайн) технологий от 2 декабря 2004г.

## Принципы норм международного права, регулирующих функционирование сети Интернет (часть из них провозглашена «Декларацией о свободе общения в Интернет»)

1. не накладывать ограничения на содержание информации в сети Интернет;
2. поощрять саморегуляцию содержания информации в сети Интернет (и ПО, которые складываются между субъектами в интернете);
3. воздержаться от использования блокировок и фильтров, которые препятствуют доступу к информации, кроме фильтров не допускающих к информации уязвимые группы, например, детей к некоторым Интернет-сайтам;
4. воздержаться от использования регистрационных схем, которые ограничивают оказание услуг через сети Интернет;
5. убрать препятствия, мешающие обеспечить доступ к сети Интернет или создание и функционирование интернет-сайтов для отдельных слоев общества;
6. не обязывать провайдеров проводить мониторинг всей информации проходящей через их сервер;
7. гарантировать право на анонимность;
8. защищать права потребителей;
9. не ограничивать движение товаров и услуг, возможность осуществления экономической деятельности, заключение сделок;
10. создать основы и гарантии справедливого разбирательства по спорам.

# Законодательное регулирование и саморегулирование в РФ

---

## Что есть?

Несколько направлений регулирования:

1. Авторские и смежные права, ТЗ.
2. Защита информации.
3. Электронная коммерция.

## Что хотят сделать?

1. Проект Президента РФ Федеральный закон (проект № 559740-5) о внесении поправок в гл.28 УК  
Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.
2. Внесение изм. в ч.4 ГК.
3. «Новое» (?) законодательство по защите персональных данных.
4. «Антиспам» законодательство.
5. 3-н «Об интернете»

## Что необходимо сделать?

- 1. ЗАКРЕПИТЬ ПРАВОВОЙ СТАТУС СУБЪЕКТОВ ИНТЕРНЕТ-ОТНОШЕНИЙ.**
- 2. САМОРЕГУЛИРОВАНИЕ.**
- 3. UDRP И АНАЛОГИЧНЫЕ ВНЕСУДЕБНЫЕ ПРОЦЕДУРЫ РАЗРЕШЕНИЯ СПОРОВ.**



## ЧЕМ ПОЛЕЗЕН ЕВРОПЕЙСКИЙ ОПЫТ ?

- 1) Умение субъектов интернет-деятельности объединяться вокруг насущных проблем интернет-бизнеса.
- 2) Объединения выступают как площадки для эффективного взаимодействия и защиты всего бизнеса, а не отдельных индивидов.

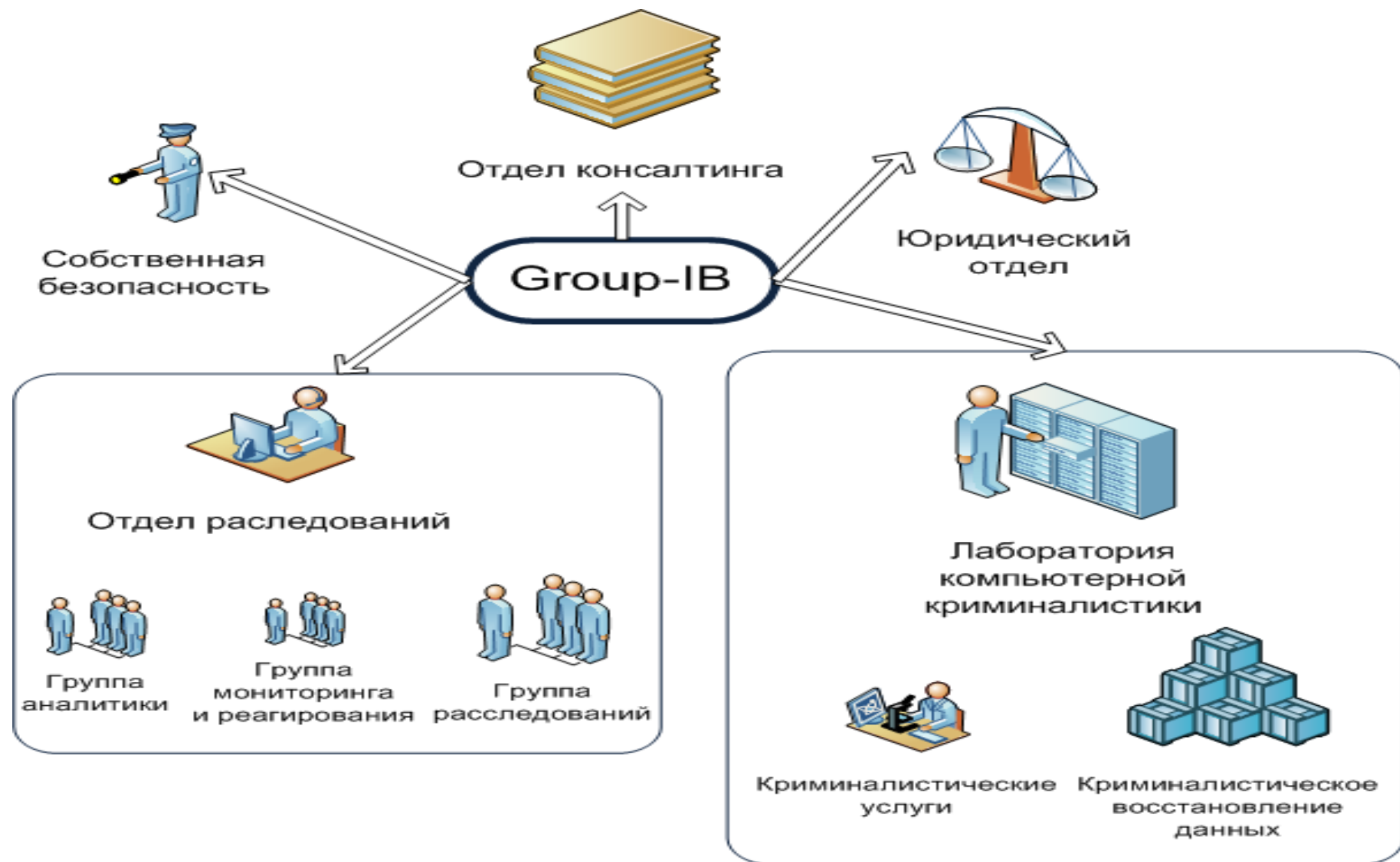
# SPAMHAUS

«Две стороны одной медали»



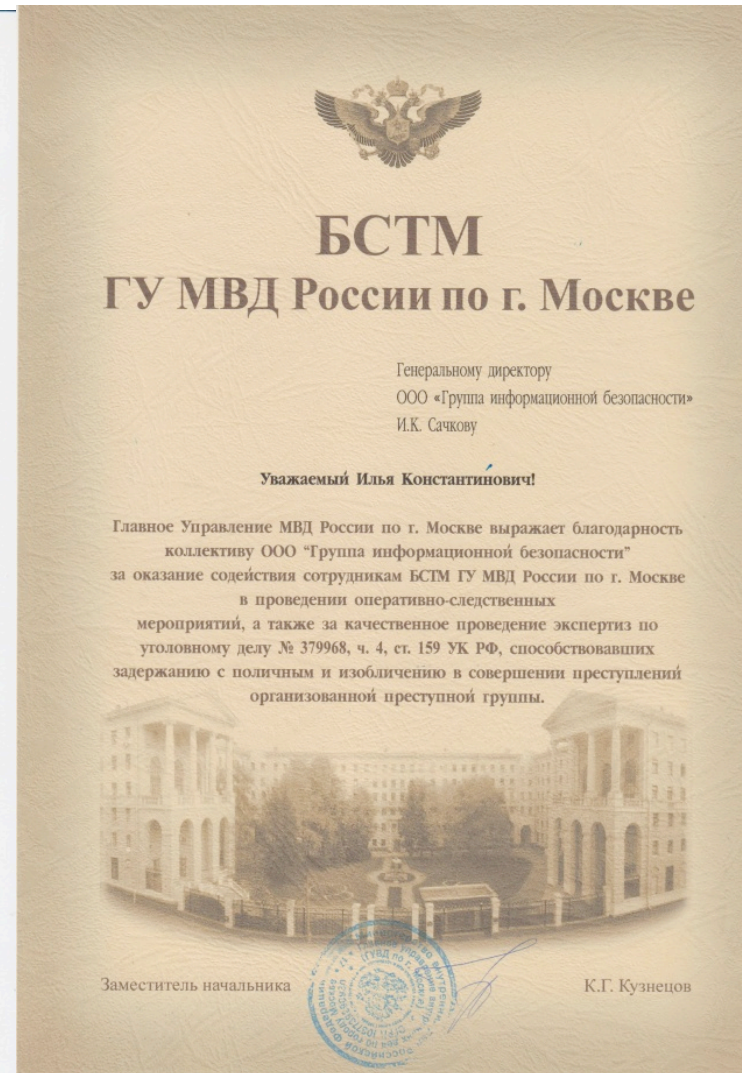
- ✓ **Первая и единственная негосударственная компания в РФ, оказывающая комплексные услуги консалтинга в области расследования инцидентов информационной безопасности**
- ✓ **Основана в 2003**
- ✓ **Сотрудничество с экспертными организациями в 48 странах**
- ✓ **24/7 мониторинг и поддержка**






- ✓ Группы по реагированию на инциденты (CERT) в 48 странах мира
- ✓ Антивирусные компании
- ✓ Производители решений по компьютерной криминалистике и информационной безопасности
- ✓ Университеты США и Европы
- ✓ Международные организации по компьютерной криминалистике
- ✓ Ассоциация сертифицированных специалистов по борьбе с мошенничествами (ACFE)
- ✓ Центры изучения угроз информационной безопасности





 Открытое акционерное общество "Российский Сельскохозяйственный банк"  
(ОАО "РОССЕЛЬХОЗБАНК")

Госконный переулок, д. 3, Москва, 119034  
Тел.: (495) 363-02-90, факс: (495) 363-02-76  
Телек: 485493 R5B RU, Swift: ROSSELKHOZ, E-mail: office@roselk.ru  
ОКПО 52750822, ОГРН 1027700342890  
ИНН / КПП 772514488 / 987950001

20 января 2011 года № 16-0-102/58

Генеральному директору компании  
"Группа информационной  
безопасности - Group-IB"


И.К.Сачкову

107023, Москва, Мажоров переулок,

 КОММЕРСИАЛЬНЫЙ  
СДМ  
ОТКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО

КБ «СДМ-БАНК» (ОАО)  
125424, Москва, Волоколамское шоссе, 73  
Тел.: (495) 705-90-90, 490-15-45, факс: (495) 490-65-09  
Телефакс: 911096 SDM-RU  
ИНН 7733043350  
Корр. сч. 30101810600000000685, БИК 044583685  
SWIFT CODE SJSCRUMM  
E-mail: post@sdm.ru, www.sdm.ru  
27 июля 2009 № 4453/1100000

На № \_\_\_\_\_ от \_\_\_\_\_

 СМП БАНК

Адрес: Садовническая ул. д. 27, стр. 1  
Москва, Россия, 105221  
Телефон: +7 495 36 18 18  
Факс: +7 495 36 18 18  
E-mail: info@smpbank.ru

ОГРН: 1027700145  
ИНН: 77021545  
КПП: 7702101

На № \_\_\_\_\_ от \_\_\_\_\_ 107023, Москва.

 СОБИНБАНК  
РАЗУМНЫЙ ВЫБОР

28 ЯНВ 2011 № 6А-5-19/239114

Генеральному директору  
Group-IB  
г-ну Сачкову И.К.

Уважаемый Илья Константинович!

Коллектив Департамента безопасности ОАО «Собинбанк» выражает признательность за вклад Вашей компании Group-IB в дело обеспечения информационной безопасности ОАО «Собинбанк». Благодаря сотрудничеству с компанией Group-IB нам удалось предотвратить ряд инцидентов информационной безопасности, а так же провести расследования имевших место быть инцидентов.

Департамент безопасности ОАО «Собинбанк» надеется на дальнейшее успешное сотрудничество с компанией Group-IB в интересах обеспечения безопасности Банка, наших Клиентов и Партнеров.

Начальник Департамента безопасности  
ОАО «Собинбанк»

27.01.2011

 А.Н. Косарев

 Swedbank

ОАО «Сведбанк»  
125047, Москва, ул. Лесная, д. 5  
Телефон, факс  
+7 495 777 6363  
+7 495 777 6364  
www.swedbank.ru  
Лицензия Банка России №3054  
БИК 044579893 ОГРН 1027739331529  
ИНН 7734051393 КПП 775001001

Генеральному директору  
ООО «Группа Информационной  
безопасности»  
САЧКОВУ И.К.


Уважаемый Илья Константинович!

От лица ОАО «Сведбанк» и от себя лично благодарю Вас и Вашу компанию за активное содействие в борьбе с киберпреступностью. Наш банк искренне желает Вам процветания, успеха в делах и финансового благополучия, и надеется на дальнейшее плодотворное сотрудничество.

Начальник Управления  
риск-менеджмента,  
член Правления

 В.Г. Логофет

Исполнитель: Трубинова А.А.  
Тел.777-6363 (доб. 1476)

 УРАЛСИБ | БАНК

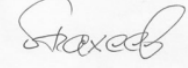
www.bankuralsib.ru

Генеральному директору  
компании Group-IB  
Сачкову И. К.

Уважаемый Илья Константинович!

От имени Департамента информационной безопасности ОАО «УРАЛСИБ» выражаю благодарность специалистам компании Group-IB - Александру Фоминенкову, Андрею Колтакову, Дмитрию Васильеву за выполнение работ по выявлению уязвимостей в корпоративной информационной системе с надлежащим качеством и точно в срок. Проведенные тесты на проникновение в корпоративную информационную систему помогли выявить уязвимости в программном обеспечении, что позволило оперативно внести соответствующие изменения и повысить уровень защищенности разрабатываемой информационной системы. Надеемся на дальнейшее эффективное взаимовыгодное сотрудничество с компанией Group-IB.

Руководитель Департамента  
информационной безопасности

 А.В. Чаев

04.07.2011г.

Открытое акционерное общество «БАНК УРАЛСИБ»

Ефремова, Е. Москва, Россия, 119048  
Тел: (495) 725-90-29, (495) 785-12-12, факс: (495) 745-75-10  
ОКПО 30202914 ОГРН 1020290001950 ИНН/КПП 5027406211/5987950001 БИК 044525787  
Корр. сч. 30101810100000000787 в ОПЕРУ Московского ГТУ Банка России г. Москва



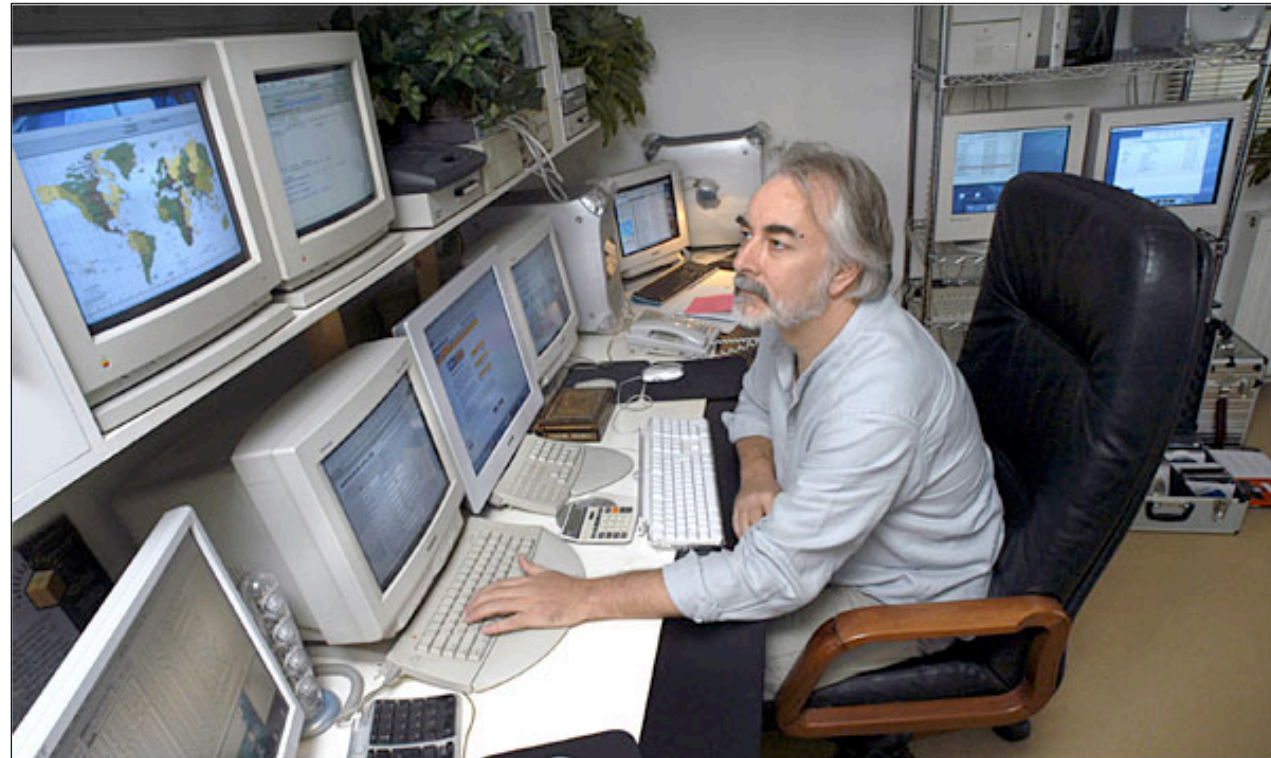
# КТО СТОИТ ЗА SPAMHAUS?





# Биографическая справка

- ✓ основана в 1998 году
- ✓ учредитель – Стив Линфорд
- ✓ обилие спонсоров (телекомы, хостинги и др.)
- ✓ и т.д.



INVESTIGAT

# Внутренняя кухня

## Анти-спам листы:

- ✓ SBL (Spamhaus Blocklist)
- ✓ XBL (Exploits Blocklist)
- ✓ PBL (Policy Blocklist)
- ✓ DBL (Domains Blocklist)
- ✓ DROP (Don't Route or Pear)
- ✓ ROKSO (Registry of known Spam operators)



## IP адрес заподозрен в рассылке СПАМа

1. Spamhaus добавляет данный адрес в одну из своих баз данных. Часто, в базы данных определяют и весь класс адресов, сопряженных с данным адресом.

- SBL - Spamhaus Block List
- XBL - Exploits Block List
- PBL - Policy Block List
- DBL - Domain Block List
- ROKSO - Register of Known Spam Operations
- DROP - Don't Route Or Peer

2. Spamhaus контактирует с организмом, отвечающим за вовлеченный IP адрес или диапазон адресов - обычно это интернет или хостинг провайдер - требуя прекращения работы ресурсов сервера, заподозренного в причастности к спам-рассылкам.

2а. Положительный ответ провайдера означает блокировку всей Интернет активности ресурса, занесенного в базы данных Spamhaus.

2б. В случае отрицательного ответа на требования Spamhaus - см. п.3

2с. Spamhaus добавляет в свои базы данных весь диапазон адресов, подконтрольный нерадивому провайдеру - как организации, способствующей СПАМ-деятельности.

3. Spamhaus обращается к вышестоящему организму, ответственному за вовлеченный IP-адрес и весь диапазон адресов нерадивого провайдера, дерзнувшего ответить отказом на требование отключить IP-адрес, подозреваемый в рассылке спама, с требованием блокировки всех вышеперечисленных ресурсов.

3а. В случае положительного ответа, блокируется как изначально подозреваемый IP-адрес, так и весь диапазон, контролируемый организмом, отказавшимся сотрудничать со Spamhaus.

3б. В случае отрицательного ответа, Spamhaus идет дальше вверх по иерархической лестнице администрирования Интернет-ресурсов, требуя наказания для отказавшей в сотрудничестве стороны.

3с. Spamhaus добавляет в свои базы данных весь диапазон адресов, подконтрольный данному организму - как организации, способствующей СПАМ-деятельности.



# Скандальные дела и Spamhaus

## Война с e360 Insight LLC



**NIC.AT**

**SPAMWISE**

**NIC.LV**

**GOOGLE**



# Российский опыт и SPAMHAUS

## AGAVA

AGAVA	
<u>81.177.1.51</u>	<u>81.177.1.70</u>
<u>81.177.1.52</u>	<u>81.177.1.71</u>
<u>81.177.1.53</u>	<u>81.177.1.72</u>
<u>81.177.1.54</u>	<u>81.177.1.73</u>
<u>81.177.1.55</u>	<u>81.177.1.74</u>
<u>81.177.1.56</u>	<u>81.177.1.75</u>
<u>81.177.1.57</u>	<u>81.177.1.76</u>
<u>81.177.1.58</u>	<u>81.177.1.77</u>
<u>81.177.1.59</u>	<u>81.177.1.78</u>
<u>81.177.1.60</u>	<u>81.177.1.79</u>
<u>81.177.1.61</u>	<u>81.177.1.80</u>
<u>81.177.1.62</u>	<u>81.177.1.81</u>
<u>81.177.1.63</u>	<u>81.177.1.82</u>
<u>81.177.1.64</u>	<u>81.177.1.83</u>
<u>81.177.1.65</u>	<u>81.177.1.84</u>
<u>81.177.1.66</u>	<u>81.177.1.85</u>
<u>81.177.1.67</u>	<u>81.177.1.86</u>
<u>81.177.1.68</u>	<u>81.177.1.87</u>
<u>81.177.1.69</u>	...

SPAMHAUS	
<u>64.4.205.84</u>	<u>209.85.133.137</u>
<u>58.65.236.209</u>	<u>74.125.47.255</u>
<u>79.135.161.10</u>	<u>72.14.207.0</u>
<u>211.94.190.7</u>	<u>72.14.192.0</u>
<u>212.68.146.240</u>	<u>209.85.129.0</u>
<u>207.234.225.114</u>	<u>72.14.207.191</u>
<u>200.196.228.18</u>	<u>72.14.203.118</u>
<u>200.205.125.100</u>	<u>66.249.83.0</u>
<u>64.233.183.0</u>	<u>72.14.207.0</u>
<u>209.85.218.0</u>	<u>72.14.207.118</u>
<u>66.249.91.113</u>	<u>72.14.204.0</u>
<u>66.249.91.102</u>	<u>58.65.238.0</u>
<u>66.249.91.101</u>	<u>58.65.239.27</u>
<u>66.249.91.100</u>	<u>58.65.238.42</u>
<u>74.125.0.0</u>	<u>58.65.239.154</u>
<u>209.85.217.255</u>	<u>58.65.237.137</u>
<u>74.125.45.101</u>	<u>58.65.239.66</u>
<u>209.85.133.191</u>	<u>58.65.238.18</u>
<u>72.14.252.0</u>	...

## Majordomo

## RU-CENTER



если бы я был судьей, я бы приговорил всех сотрудников и владельцев спамхауса посадить на кол  
эти ублюдки палят спам-рассылку и банят сразу провайдерскую подсеть, требуя с прова плату за снятие бана. но ведь пров-то объективно не виноват, что хостер поставил пхп-бб или впервые в жизни написанную самопальную мегагостевуху.

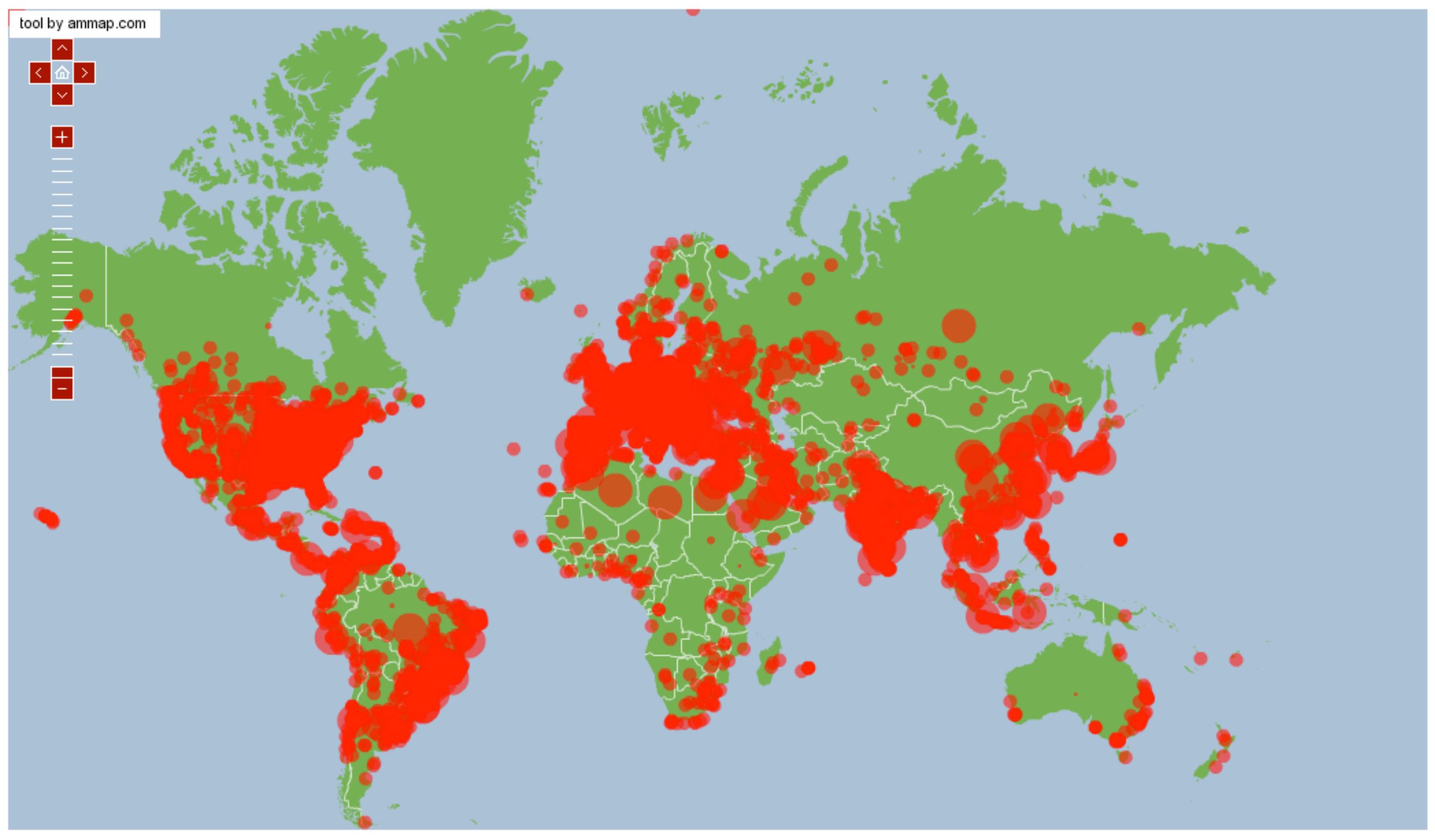
Русскоязычный пример недовольства методами работы Spamhaus

YET... They list VistaPrint.... You guys are abosolutely 100% verifiably retarded. I can't believe Yahoo! uses such a lying, deceiving, bribe taking SPAM company. Who knew Spamhaus profited from Spam? Just check any shoeshoe RBL... Some of their "resolved" listings are still quite active and spewing money making spam for the "oh-so-great" spamhaus.

You people are blind.

Англоязычный пример недовольства деятельностью Spamhaus

tool by ammap.com



ESTIGAT

# Вопросы?



Андрей Комаров

[komarov@group-ib.ru](mailto:komarov@group-ib.ru)





Встречи объединяют!

to be continued ...  
продолжение следует...

*София Александровна Грунюшкина  
Генеральный Директор «Инфоэкспертиза»,  
преподаватель дисциплин:  
«Расследование правонарушений в СКИ»,  
НИЯУ «МИФИ»  
Конт: skype: sofya\_guru, email: guru2003@list.ru*