



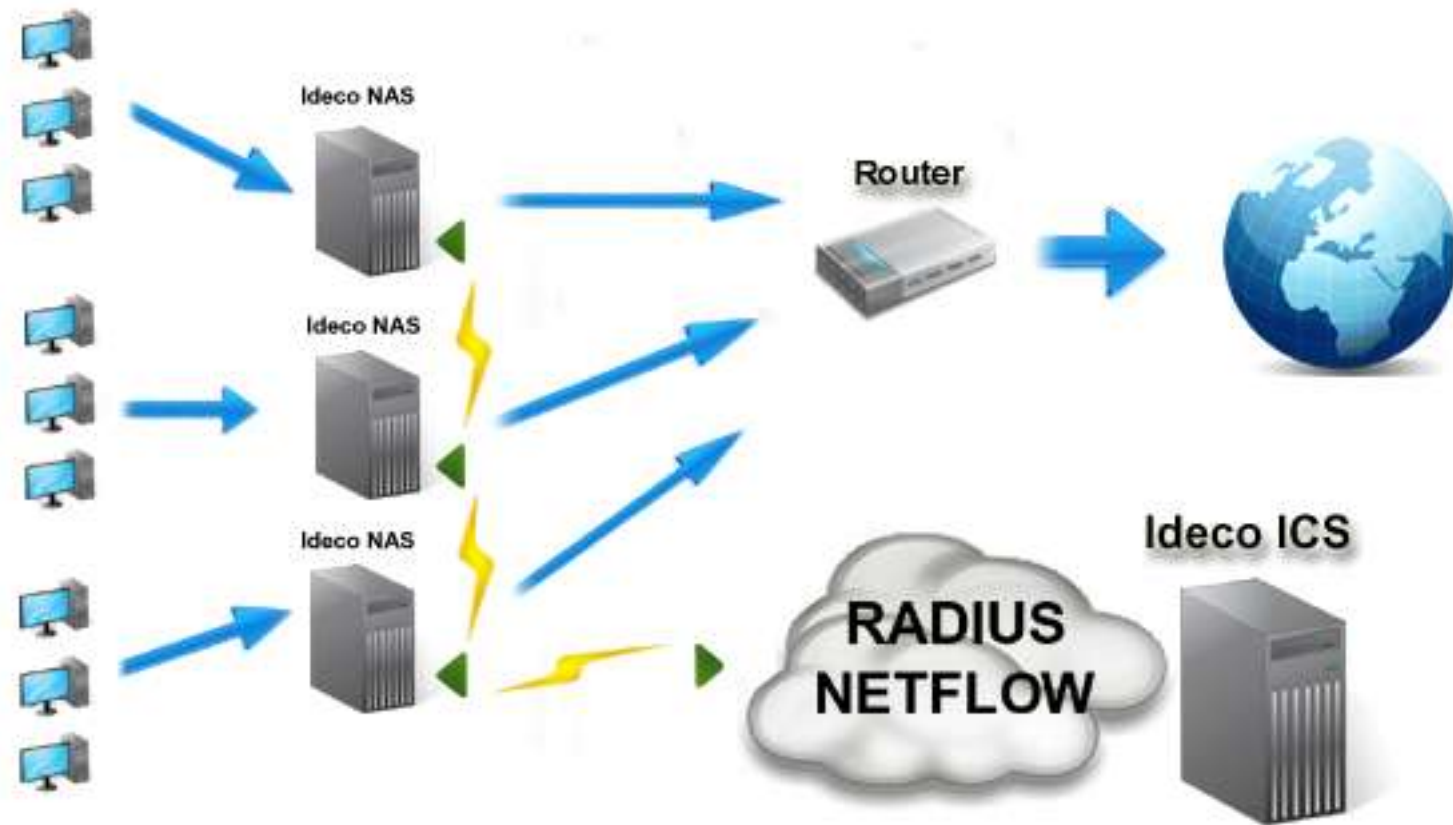
# Интернет-шлюз Ideco ICS: центр управления пакетами и потоками трафика

# Компания «Айдеко»



- Год основания - 2005
- Специализация: разработка сетевого инфраструктурного ПО
- Количество сотрудников – 30 человек
- Офис разработки и продаж – Екатеринбург
- Более 5000 пользователей в России, странах СНГ, Германии, Китае, Польше, Чехии

# АСР Ideco – сертифицированный биллинг



# SkyDNS – первый облачный сервис защиты

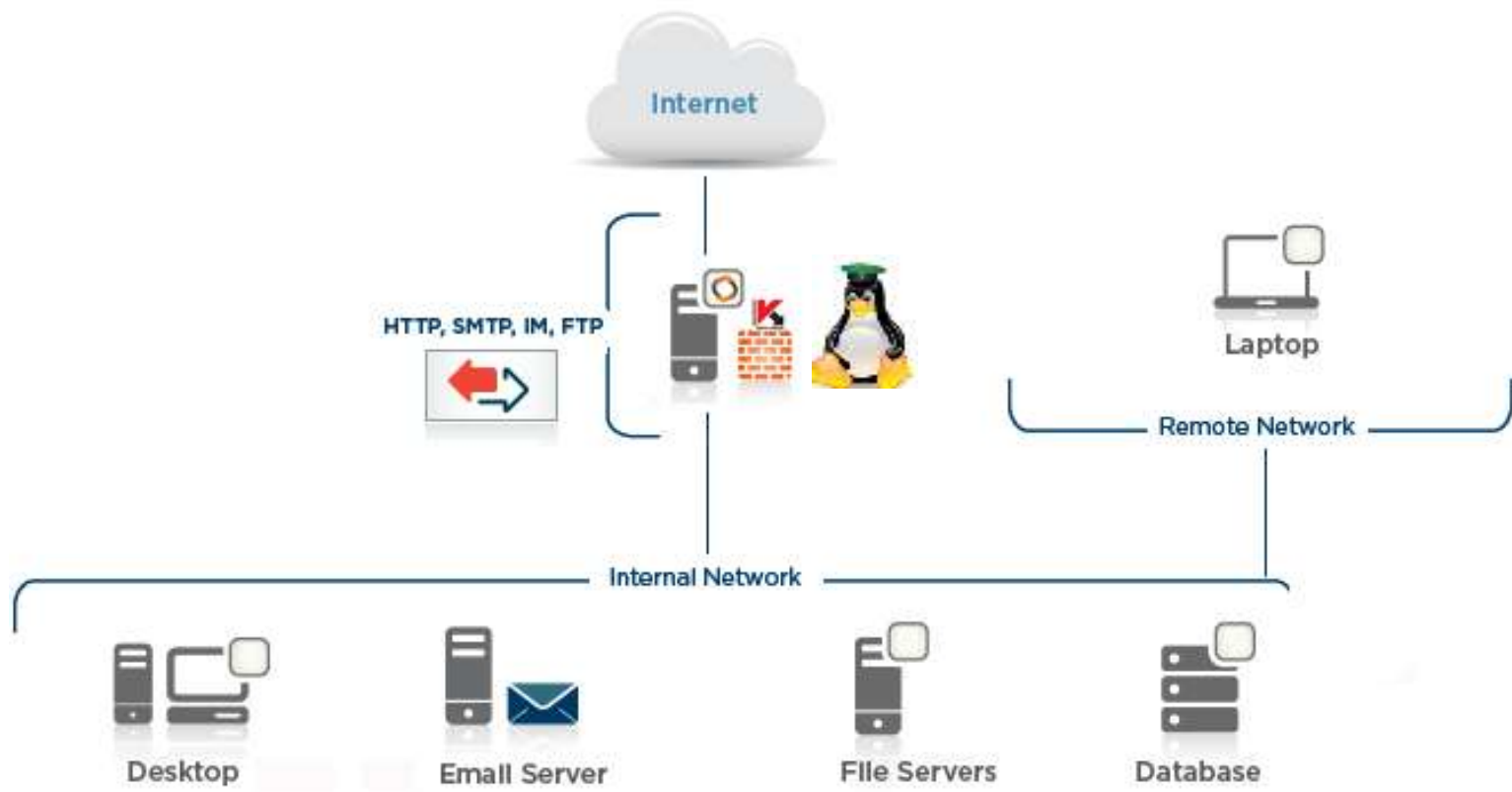


- 4 дата-центра
- 60 категорий непродуктивных и опасных сайтов
- миллионы URL в базе данных
- free&use



A composite image showing the SkyDNS website interface and a SkyDNS Agent window. The website displays the SkyDNS logo, navigation tabs for 'Доступ', 'Фильтр', and 'Исключения', and sections for 'Черные сайты' and 'Сайты для взрослых'. The SkyDNS Agent window shows the current IP address as 109.197.228.95 and a status message: 'Интернет под контролем'. It also includes a login form with fields for 'E-mail учетной записи' (mail@skydns.ru) and 'Пароль', and 'OK' and 'Отмена' buttons.

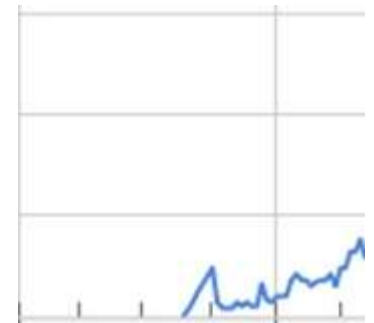
# Idecos ICS: центр управления трафиком



# Утро одного понедельника 10:00

Марина, менеджер отдела по работе с персоналом:

*«..господин сетевой инженер, уже двое наши сотрудников перешли работать к основному конкуренту, может придумаете, что-нибудь такое, чтобы ни у кого не было доступа к страничке вакансий конкурента. А может быть, вообще его их удалить. Пожалуйста, ну придумайте что-нибудь..»*

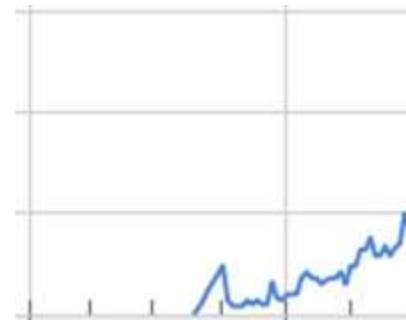


# Утро одного понедельника 10:55



Жанна, менеджер учебного центра:

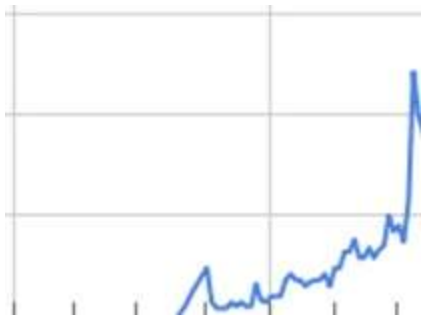
*«..извини, что по делу, но вопрос срочный, генеральный решил узнать всех лодырей, кто за месяц ни разу не открывал наш «Портал новых знаний», у нас такой статистики не велось, может ты в свой мониторчик посмотришь, по айпишникам там или еще как-нибудь, у тебя же все равно все ходы записаны? Ну очень надо, помоги, pls ..»*



# Утро одного понедельника 12:00

Игорь Маратович, директор по общим вопросам:

*«..к конкурентам бегают, на компьютерах черти-что хранится, вчера у всех менеджеров откуда-то маркетинговый план появился. У серьезных людей с конфидентом порядок, одни мы как дети, ничего не контролируем и никого не выявляем. Слушай, старик, если ты к концу квартала с безопасностью порядок не наведешь – делай выводы».*



# Утро одного понедельника, итоги

**3 новых задачи:**

**1 срочная**

**1 проектная**

**1 процессная**

**Чем больше процессных задач, тем меньше времени остается на проектную работу**

**Боссы ценят проекты, а не процессы.**



*Коллективное бессознательное: системное администрирование – это непыльная, но интересная работа. В части сетевых дел – системный администратор всемогущ.*



# Ideco ICS: шлюз всемогущий

простота&защищенность&экономия



Логин:

Пароль:

# Ideco ICS: центр управления трафиком

 <b>Пользователи</b> Всего пользователей: 227 Подключено: 172	 <b>Монитор</b> Активных процессов: 4 Памяти свободно: 1119 Мб Свободно места HDD: 27.54 Гб Всего места на HDD: 57.12 Гб <a href="#">Подробнее</a>	 <b>Управление сервером</b> Системное время: 12:08:08 Системная дата: 16.03.2011 Прокси: ✓ DHCP: ✓ <a href="#">Подробнее</a>	 <b>Безопасность</b> Пресечено попыток сканирования портов: 11321 Пресечено вспышек вирусной активности: 0 Пресечено угроз SPAM-рассылок: 0	 <b>Антивирус</b> Найдено вирусов в почте: 45 Найдено вирусов в web: 74 Обновление антивируса Касперского: 16:04 18.02.2011 Антивирус Касперского Почта: ✓ <a href="#">Подробнее</a>
 <b>Антиспам</b> Писем всего: 1206751 Из них чистых: 192846 Обнаружен спам: 1013905 Антиспам Касперского: ✓ <a href="#">Подробнее</a>	 <b>Почтовые правила</b> Фильтров отправителя: 0 Фильтров получателя: 2 Фильтров текста: 2 Фильтров заголовка: 4	 <b>Контент-фильтр</b> Состояние: ✓ Категорий фильтра: 7 Всего категорий: 23	 <b>Помощь</b>	 <b>Выход</b>

Не отображать при следующем входе  
Вернуть отображение обзорной панели можно в разделе Сервер→Дополнительно→Опции

# Ideco ICS: проще простого

The screenshot displays the Ideco ICS 4 web interface. At the top left is the Ideco logo and the text 'Интернет-шлюз Ideco ICS 4'. A navigation bar contains icons and labels for 'Пользователи', 'Монитор', 'Безопасность', 'Сервер', 'Профили', 'О программе', and 'Выход'. Below this is a tabbed interface with tabs for 'Общие', 'Почта/IM/BB', 'Ограничения', 'Статистика', and 'Финансы'. The 'Общие' tab is active, showing configuration for user ID 24. On the left is a tree view of the user directory, with 'Администратор Иванов Сергей Юрьевич' selected. The main configuration area includes fields for 'Пользователь' (Администратор Иванов Серг), 'Логин' (adminsergey), 'Профиль' (Основной тариф), and 'IP-адрес' (10.128.0.9). There are also checkboxes for 'NAT', 'Постоянно подключен', 'Разрешить VPN из интернет', 'Администратор технический', 'LDAP/AD пользователь', and 'Разрешить переподключение'. A 'Сохранить' button is at the bottom.

# Ideco ICS: проще простого

Статистика по посещаемости top 100

Год: 2011 ▼ Месяц: Март ▼

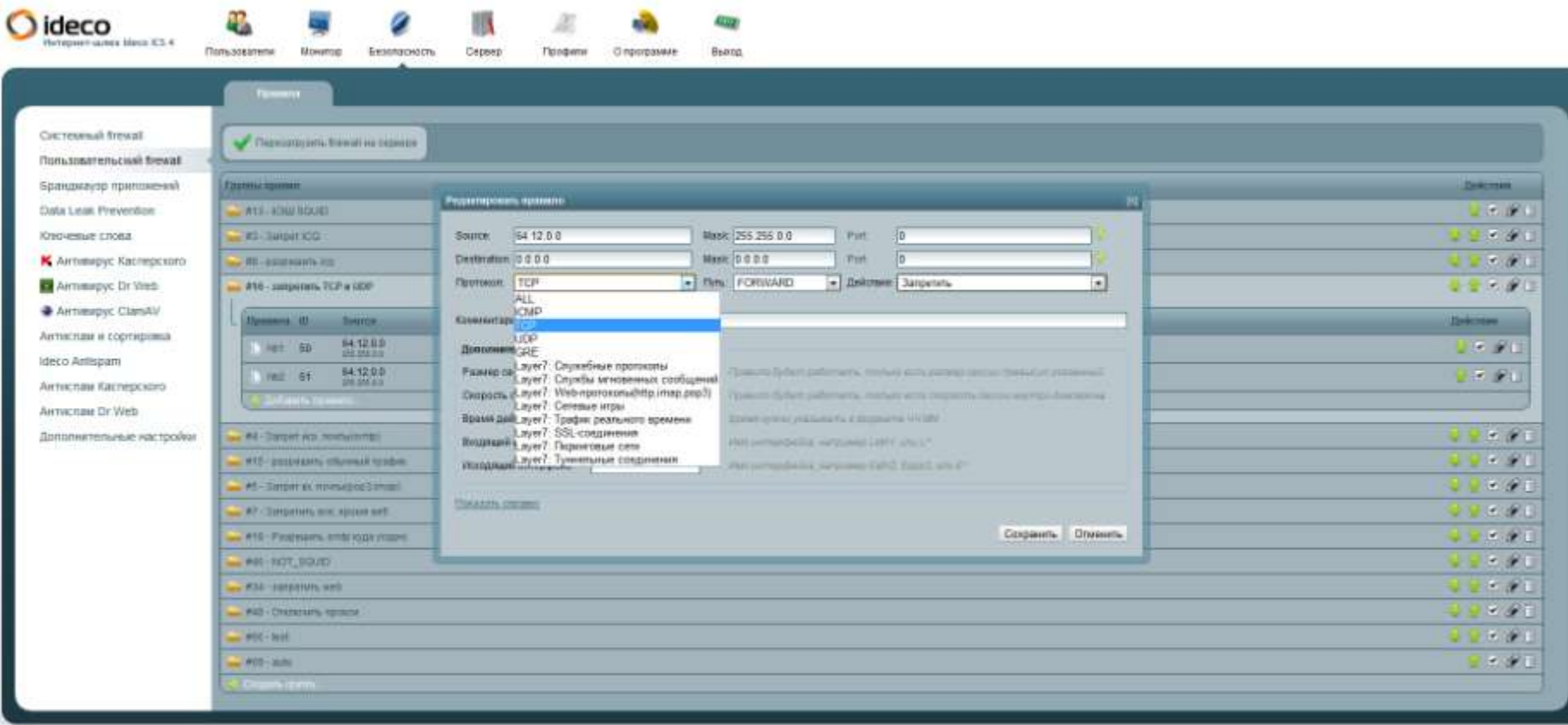
Подробная статистика посещений за месяц

Период: 01.01.1970 05:00  по 01.01.1970 05:00

▼ IP адрес:   подробно по времени

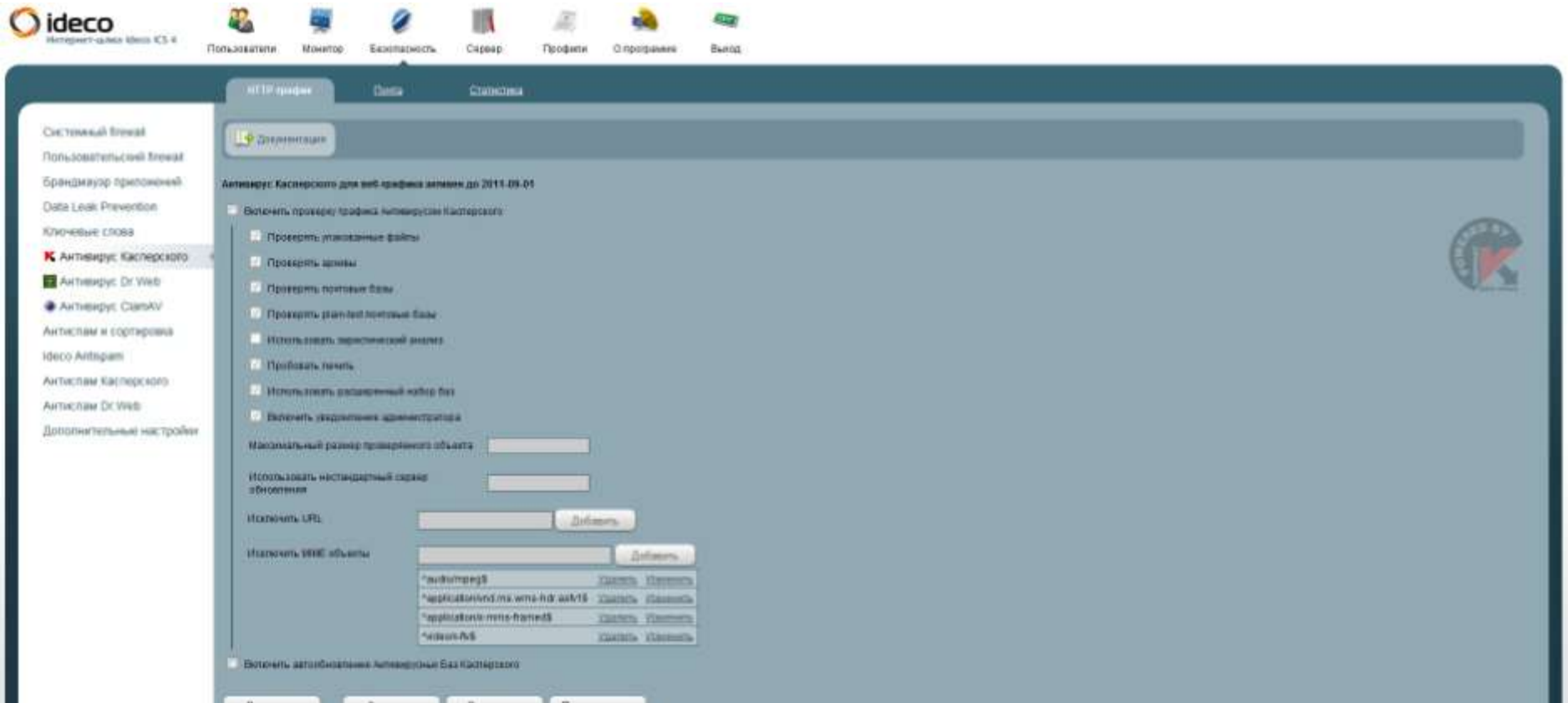
Дата	Адрес	Объем байт.	Направление	Протокол	Описание
	84.252.151.5	13,645,975	Входящий		
	87.248.210.254	13,032,519	Входящий		cdn-87-248-210-254.lon.llnw.net
	87.242.77.160	13,073,427	Входящий		test.ura.ru
	87.250.251.64	12,712,015	Входящий		webattach.mail.yandex.net
	8.27.5.126	9,409,463	Входящий		
	173.194.18.11	10,032,127	Входящий		
	193.9.17.3	10,489,370	Входящий		N3.hosterov.ru
	95.169.190.32	10,262,979	Входящий		ns.km35325.keymachine.de
	217.106.225.150	10,443,221	Входящий		barbero-8.m-10.ru

# Ideco ICS: проще простого



# Ideco ICS: безопасности много не бывает

NAT DLP 2 межсетевых экрана 3 антивируса 4 анти-спама  
18 категорий фильтрации количество своих правил - unlim



# Ideco ICS: безопасности много не бывает

Модуль dlp (data leakage prevention) обеспечивает защиту от утечек конфиденциальных документов путем сопоставления объектов в исходящем трафике с эталонными отпечатками

Системный firewall  
Пользовательский firewall  
Брандмауэр приложений  
**Data Leak Prevention**  
Ключевые слова  
Antivirus Касперского  
Antivirus Dr.Web  
Antivirus ClamAV  
Антиспам и сортировка  
Ideco Antispam  
Антиспам Касперского  
Антиспам Dr.Web  
Дополнительные настройки

В этом разделе отображаются данные, перехваченные DLP-фильтрами. Каждая строка таблицы соответствует одному соединению. Щелкнув по строке соединения можно увидеть дополнительные подробности. (закрыть)

ID	Дата	Пользователь	IP	Имя	Размер	Действия
425	16.02.2011 - 16:50	Крулик Артем	10.80.1.16	POST http://sachin-one.ru/dp/rtloader.php HTTP/1.1	16.61 Kb	[Иконка]
424	16.02.2011 - 16:50	Крулик Артем	10.80.1.16	POST http://sachin-one.ru/dp/rtloader.php HTTP/1.1	16.61 Kb	[Иконка]
423	16.02.2011 - 16:50	Крулик Артем	10.80.1.16	POST http://sachin-one.ru/dp/rtloader.php HTTP/1.1	0 Kb	[Иконка]
422	16.02.2011 - 16:54	Крулик Артем	10.80.1.16	POST http://sachin-one.ru/dp/rtloader.php HTTP/1.1	0.1 Kb	[Иконка]
421	16.02.2011 - 14:01	nvkay	10.80.1.75	POST http://img.3dchess.net/upload-image HTTP/1.0	0.1 Kb	[Иконка]
420	16.02.2011 - 14:01	nvkay	10.80.1.75	POST http://img.3dchess.net/upload-image HTTP/1.0	0.08 Kb	[Иконка]
419	16.02.2011 - 13:58	nvkay	10.80.1.75	POST http://img.3dchess.net/upload-image HTTP/1.0	0.07 Kb	[Иконка]
418	16.02.2011 - 13:58	nvkay	10.80.1.75	POST http://img.3dchess.net/upload-image HTTP/1.0	0.08 Kb	[Иконка]
417	16.02.2011 - 11:27	Обуев Владимир	10.80.1.57	POST http://w2geo.mobile.yandex.net/getlocation HTTP/1.1	649 z	[Иконка]
415	16.02.2011 - 11:36	Александра Ушакова	10.80.1.87	Stat.creal@mail.ru	700.89 Kb	[Иконка]
416	16.02.2011 - 11:34	Александра Ушакова	10.80.1.87	Stat.creal@mail.ru	700.88 Kb	[Иконка]
414	16.02.2011 - 11:34	Александра Ушакова	10.80.1.87	Stat.creal@mail.ru	700.89 Kb	[Иконка]
413	16.02.2011 - 11:34	Александра Ушакова	10.80.1.87	Stat.creal@mail.ru	700.88 Kb	[Иконка]
412	16.02.2011 - 11:34	Анастасия Романова	10.80.1.14	POST http://w2geo.mobile.yandex.net/getlocation HTTP/1.1	657 z	[Иконка]
411	16.02.2011 - 11:34	Александра Ушакова	10.80.1.87	Stat.creal@mail.ru	700.89 Kb	[Иконка]
410	16.02.2011 - 11:27	Обуев Владимир	10.80.1.57	POST http://w2geo.mobile.yandex.net/getlocation HTTP/1.1	649 z	[Иконка]
409	16.02.2011 - 11:24	Анастасия Романова	10.80.1.14	POST http://w2geo.mobile.yandex.net/getlocation HTTP/1.1	657 z	[Иконка]
408	16.02.2011 - 11:17	Обуев Владимир	10.80.1.57	POST http://w2geo.mobile.yandex.net/getlocation HTTP/1.1	649 z	[Иконка]

# Ideco ICS: безопасности много не бывает

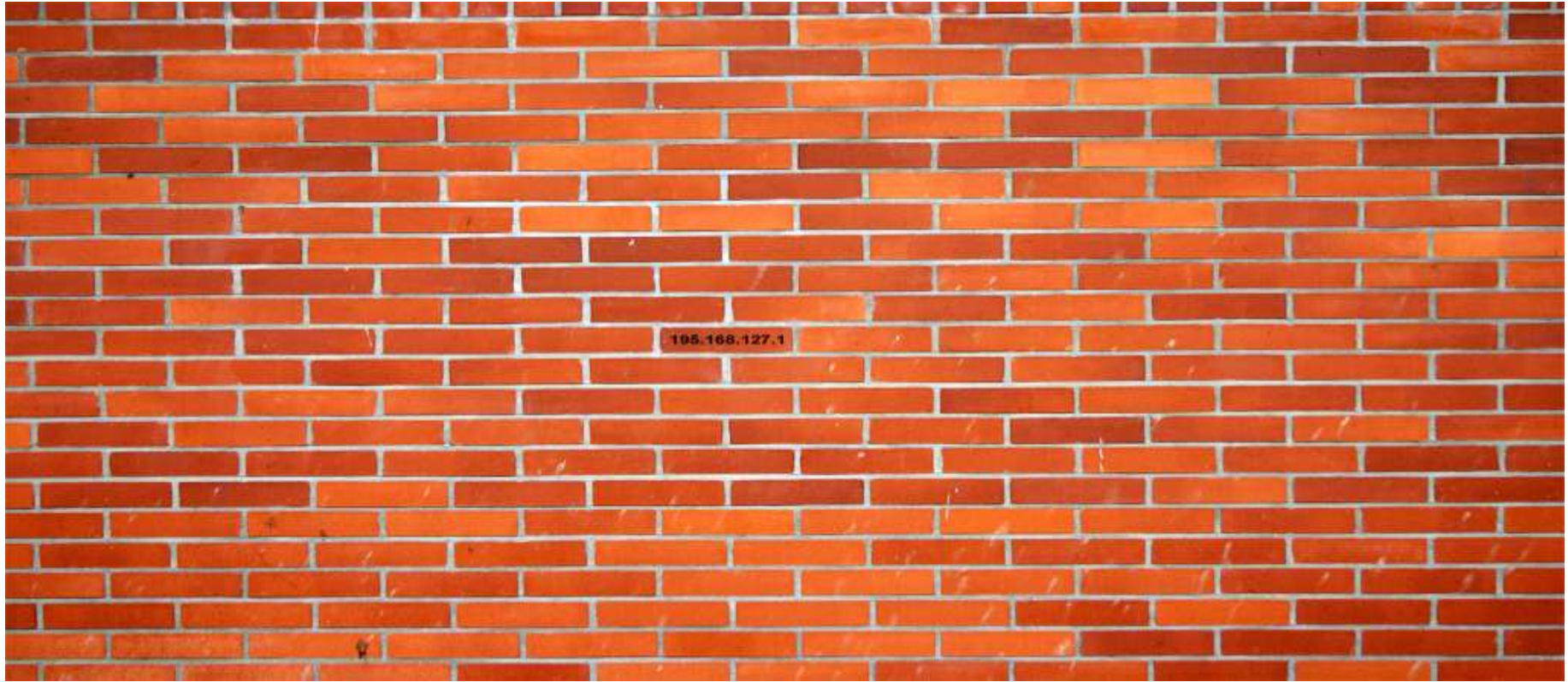
- Продукт основан на одном из самых стабильных и проверенных ядер ОС – ядре Linux 2.4
- Стандартное ядро модифицировано с целью усиления безопасности
- Технологии для беспрецедентной защищенности (chroot, read-only-run-only, нет root, NAT, защита от DOS- и DHA- атак и др)
- Используется многоуровневая система защиты
- Все внешние порты по умолчанию закрыты
- Возможность автоматического переключения при ddos
- Защита от прослушивания трафика
- Возможность шифрования любого трафика, включая внутренний
- Защита от сканеров сети и блокирование чрезмерной активности

# Idecos ICS: безопасности много не бывает



- Все сетевые службы помещены в клетки chroot, нарушение безопасности одной службы не приведет к уязвимости сервера.
- Подсистема слежения
- Запрет исполнения файлов с разделов с данными.
- Запрет монтирования новых файловых систем.
- Максимальное ограничение возможностей (capabilities) для всех служб и процессов.
- Система обнаружения и уничтожения exploit в ядре.

# Ideco ICS: безопасности много не бывает



В эти минуты и до конца воскресенья проходит очередной независимый тест на проникновение, когда для 4-5 признанных экспертов в сфере ИБ «поднимается» реальный шлюз с реальными клиентами в периметре, с реальной базой пользователей, почтовым сервером и т.д. Группа независимых хакеров пытается в течение нескольких дней, зная только внешний ip, получить доступ внутрь периметра, админские привилегии на уровне шлюза, список логинов пользователей или любую другую информацию, утечка которой будет считаться критической уязвимостью по безопасности.

# UNIX-системы неуязвимы? Миф



**Date**

Thu, 25 Nov 2010 10:57:58

**Subject**

Simple kernel attack  
using socketpair. easy,  
100% reproductiblle,  
works under guest. no way  
to protect :(

**From**

Марк Коренберг <>

Simple kernel attack using socketpair. easy, 100%  
reproductiblle,  
works under guest. no way to protect :(

See source attached.

Process become in state 'Running' but not killalble via  
kill -KILL.

eat 100% CPU, eat all available internal file  
descriptors in kernel :(

Код, приводящий к зависанию компьютера (100% загрузка всех ядер,  
исчерпание файловых дескрипторов).

<http://habrahabr.ru/blogs/linux/108835/>

# Ideco ICS: экономные инвестиции



- Не требуется дополнительный soft
- Минимум временных затрат на внедрение и обучение
- Все-в-одном решении
- Централизованный мониторинг и администрирование ИТ-инфраструктурой – стандартизация сервисов
- Консолидация серверов
- Высокий уровень автоматизации сетевого администрирования – реальное высвобождение ч/дней, до 48 в год
- Фиксированные цены (40% цен не менялись с 12.2005)
- Специальные скидки – «**Лучший выбор**» - до 30%
- Лучшее в своём классе соотношение цена/функциональность
- Kaspersky inside – эффект сокращения \$

# Ideco ICS: экономные инвестиции

## Ideco SX



Ideco SX10 – 23 700 руб.

Ideco SX20 – 33 300 руб.

Ideco SX30 – 42 900 руб.

Описание

**Характеристики**

Цены

Характеристики аппаратной платформы:

<b>Процессор:</b>	Intel® Celeron® Processor 430 (512K Cache, 1.80 GHz, 800 MHz FSB)
<b>Память:</b>	1024MB DDR-II 800MHz
<b>Жесткий диск:</b>	SATA 160GB
<b>Сетевой адаптер:</b>	PCI Acorp L-100S PCI 10/100 Mbit Realtek8139 - 2 шт.

## Ideco SMX



Ideco SMX30 – 59 800 руб.

Ideco SMX40 – 69 800 руб.

Ideco SMX50 – 77 400 руб.

Ideco SMX75 – 95 600 руб.

Описание

**Характеристики**

Цены

Характеристики аппаратной платформы:

<b>Процессор:</b>	Intel® Pentium® Processor E5500 (2,0 GHz, 800MHz 2MB)
<b>Память:</b>	2 Gb DDR2-800 SDRAM (Dual Channel, 2DIMM4)
<b>Жесткий диск:</b>	1x250GB SATA hard drive (7200rpm)
<b>Сетевой адаптер:</b>	Интегрированные Intel 82573V Gigabit Ethernet Controllers - 2шт.

# Ideco ICS: сертификат ФСТЭК России



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ  
№ РОСС RU.0001.01БИ00

## СЕРТИФИКАТ СООТВЕТСТВИЯ № 2283

Выдан 22 февраля 2011 г.  
Действителен до 22 февраля 2014 г.

Настоящий сертификат удостоверяет, что **программный комплекс межсетевой экран «Ideco ICS 3»**, разработанный ООО «Айдеко» и производимый ЗАО «Профиль Защиты» в соответствии с техническими условиями ТУ 501540-002-86201535-2010, функционирующий под управлением операционной системы Linux (kernel 2.4.24), является программным средством защиты от несанкционированного доступа к информации, не содержащей сведения, составляющие государственную тайну, соответствует требованиям руководящих документов «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1997) - по **4** классу защищенности, «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1999) - по **4** уровню контроля, технических условий и может использоваться для защиты информации в информационных системах персональных данных до **2** класса включительно.

# Idecos ICS: сертификат ФСТЭК России

ФЗ Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных"

ЗПД был принят в августе 2006 г.

Сфера действия данного закона охватывает практически все, что связано с использованием личной информации. Он регулирует отношения, связанные с обработкой персональных данных, независимо от того, кто и как ее осуществляет.

Соответствие международным нормам, прежде всего актам Европейского Союза, в которых существует дифференцированный подход к компаниям различных стран: для тех, чье законодательство обеспечивает «должную защиту» персональных данных, установлен лояльный режим деятельности в Европейском Союзе, к остальным предъявляются жесткие ограничения, и деятельность, связанная с использованием персональных данных, для них весьма затруднена. Поэтому принятие российского закона было вызвано тем, чтобы снять возможные ограничения для деятельности российских компаний.

Персональные данные – это ЛЮБАЯ информация, относящаяся физическому лицу. К ней отнесены, например, фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы. Физические лица в законе обозначены как субъекты персональных данных. Под обработкой информации понимаются все операции с персональными данными. Обработку осуществляют операторы ПДн. А сети, в которых выполняется обработка, называются информационные системы с персональными данными (ИСПДн).

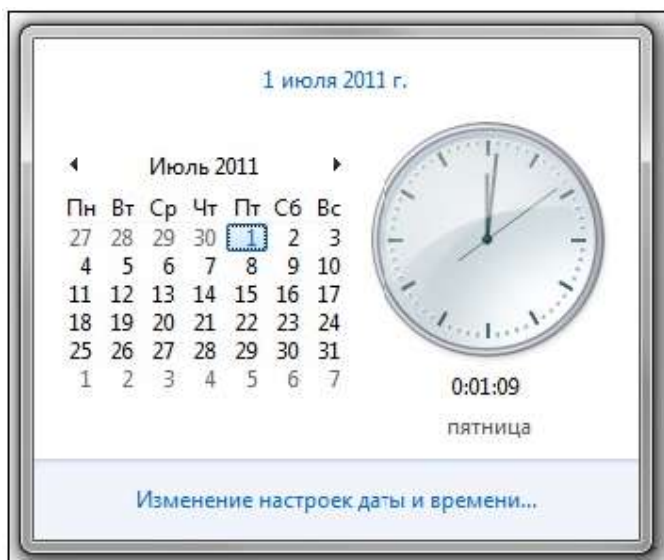
Принятие закона сопровождалось практически нулевой нормативной базой. Существовали ведомственные инструкции ФСТЭК под грифом ДСП, которые можно было получить по запросу, но эта процедура как показала практика не работала.

Поэтому на нормализацию нормативно-правовой базы был взят «небольшой» тайм-аут.

# 1 июля 2011 - осталось меньше 100 дней

В настоящее время, по разным объективным и субъективным причинам, срок действия закона Ф3-152 в части разработанных ранее ИСПДн перенесен сначала до 1 января 2011 года, а затем и до 1 июля 2011 года (закон № 444277-5). Однако все разрабатываемые (модернизированные) с начала 2011 года ИСПДн уже должны соответствовать закону.

Это означает, что операторы персональных данных, не сумевшие выполнить требования Ф3-152, с 1 января или 1 июля 2011 года могут понести соответствующую гражданскую, административную, дисциплинарную ответственность.



## 5. Определить необходимость уведомления уполномоченного органа по защите ПДн. Составить и отправить уведомление.

[www.pd.rsoc.ru](http://www.pd.rsoc.ru)

Направляем уведомление.

..подпункта 8 пункта 2 статьи 22 Федерального закона «О персональных данных», предусматривающего, что оператор вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных обработку персональных данных обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Либо подготавливаем правовое обоснование об отсутствии необходимости.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО НАДЗОРУ В СФЕРЕ СВЯЗИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МАССОВЫХ КОММУНИКАЦИЙ

# Портал персональных данных

Уполномоченного органа по защите прав субъектов персональных данных

[Главная](#) | [Об уполномоченном органе](#) | [Консультативный совет](#) | [Пресс-служба](#) | [Законодательство](#) | [Реестр операторов](#) | [Обращения граждан](#)

### Поиск по реестру

В настоящее время в реестре содержится информация о 85 524 операторах персональных данных

[Расширенный поиск](#)

### Новости и события

**[Утечка в Белом доме США: скомпрометированы данные 250 тыс. человек](#)**

08 февраля 2010 [События](#)

**[Интервью руководителя управления Роскомнадзора по Ростовской области Александра Ваганова. "Строго конфиденциально"](#)**

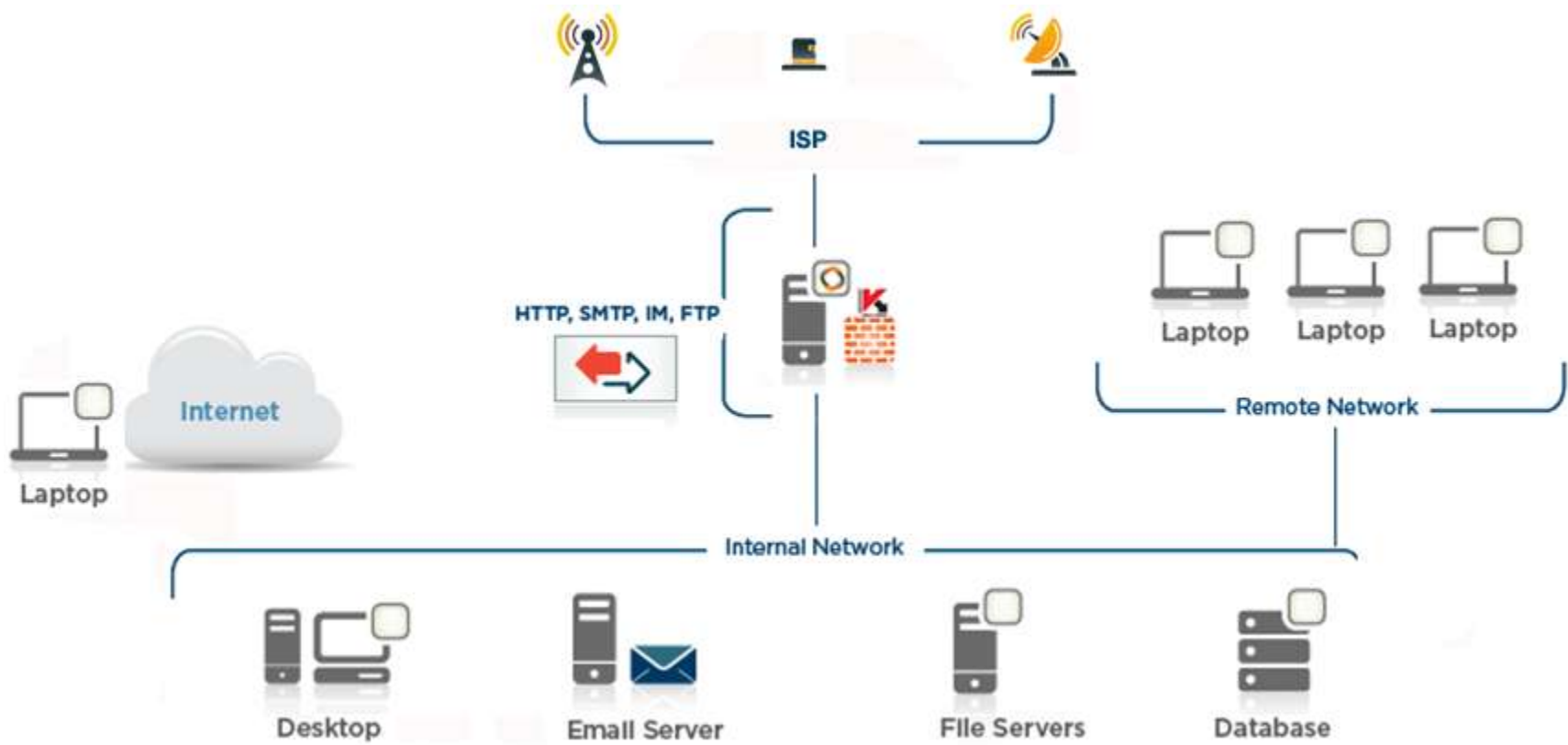
04 февраля 2010 [Публикации](#)

**[Арбитражный суд Иркутской области отказал АКБ «Радиян» в требовании признать недействительными Акт и Предписание, выданные Управлением Роскомнадзора](#)**

[Обобщенные предложения органов государственной власти и заинтересованных организаций по гармонизации законодательства в сфере персональных данных](#)

[Обновление в законодательстве](#)

# Ideco ICS:



# Ideco ICS: бизнес-преимущества



- Все сервисы – в одном решении
- Быстрое развертывание и обучение
- Высочайший уровень защиты от внешних атак
- Высокий уровень автоматизации
- Повышение продуктивности работы пользователей
- Соблюдение нормативных требований в сфере защиты персональных данных

Самые «свежие» награды Ideco ICS:

2010 - «Продукт года» российская национальная премия для наиболее перспективных разработок в области ИТ x2

2010 – Лучшие программы 2010 года по версии PC Magazine x 3

2010 – Infosecurity: первое тиражное DLP-решение для gateway



# Idecos ICS: клиенты и внедрения Q1-2011

- Гос. Заказчики
  - Правительство Пензенской области
  - Подразделения ФСБ, ФСО и МЧС
  - Новороссийская таможня
- Банки и финансы
  - Коммерческие банки «Каспий», «Эл-Банк», «Универсал-Банк»
  - СК «Согласие»
- Промышленность
  - ОАО «Ненецкая нефтяная компания»
  - ЗАО «Авиаприбор»
  - ЗАО «Русская буровая корпорация»
- Торговля
  - ЗАО «РОСТЭК-Дон» и другие 250 заказчиков

# Ideco: вперед в будущее



- Улучшенный сервис мониторинга сессий в реальном времени
- Защищенный обмен с применением ГОСТовских криптоалгоритмов
- Система архивации электронной почты
- Модуль предотвращения атак IDS/IPS
- Поддержка беспроводных устройств
- Переход на новое ядро 2.6
- Полный набор инфраструктурных решений

**>> [www.ideco.reformal.ru](http://www.ideco.reformal.ru)**

# Спасибо за внимание!

## Вопросы ?

**Компания «Айдеко», точнее:  
Компания «Консультант Безопасность»  
*Ideco ExpertPartner***