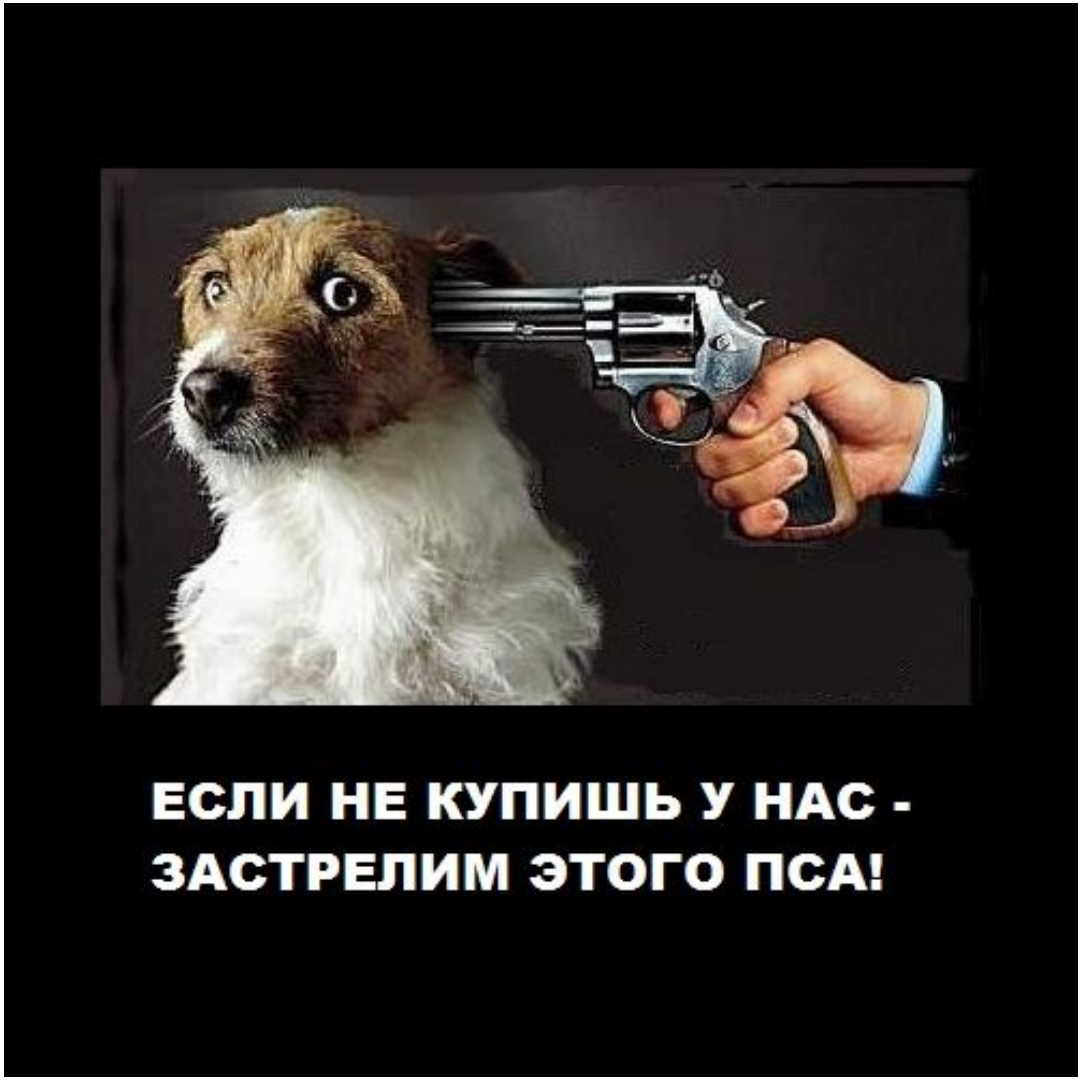
KASPERSKY lab

Лови момент, или, как не попасть в ловушку

Игорь Кошмал
Лаборатория Касперского
Представительство в СЗФО
Риланс, С.-Петербург, 27.04.2012
Igor.koshmal@kaspersky.com

Не надо назойливой рекламы!

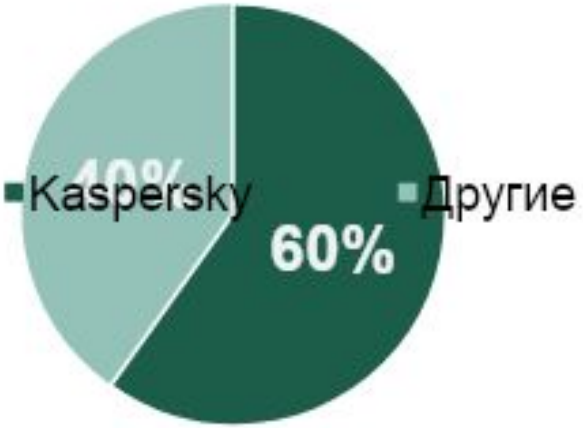


«Лаборатория Касперского»

- 14 лет на рынке

Доли рынка производителей Endpoint Security Software в России за 2010 год

Источник: IDC



Больше чем безопасность

Kaspersky LAB – на переднем краю борьбы с киберкриминалом

- **Аналитические отчеты**
- **Информация в блогах и вирусных энциклопедиях**
- **Обучающие семинары, бизнес-завтраки, конференции**
- **Образовательные программы**
- **Работа с органами власти**

Важные цифры. 2010 год

31 декабря 2010 г. –1 900 000 000* зафиксированных инцидентов

1,9 МИЛЛИАРДА!

***3700 инцидентов в секунду**

Важные цифры. 2010 год

Основные тенденции на том же уровне

В ряде технологий - переход на новый уровень

Увеличение сложности вредоносных программ

Большинство атак осуществляется через браузер

Стабилизация количества программ ~~=~~ стабилизация количества атак.

одна и та же вредоносная программа = десятки различных уязвимостей = рост количества атак.

Динамика развития информационных угроз

2011 год. Цифры.

Динамика развития информационных угроз

- 946 393 696 атаки через браузер (2 592 859 раз в день)
- сервера атак – 4 073 646 доменов в 198 странах мира

Рост по сравнению с 2010 г. – в 1,6 раза

Место	Страна	Количество атак	% от всех атак
1	США	240 022 553	25,4%
2	Россия	138 554 755	14,6%
3	Нидерланды	92 652 499	9,8%
4	Германия	82 544 498	8,7%
5	Украина	47 886 774	5,1%

Динамика развития информационных угроз

Где размещаются вредоносные ссылки

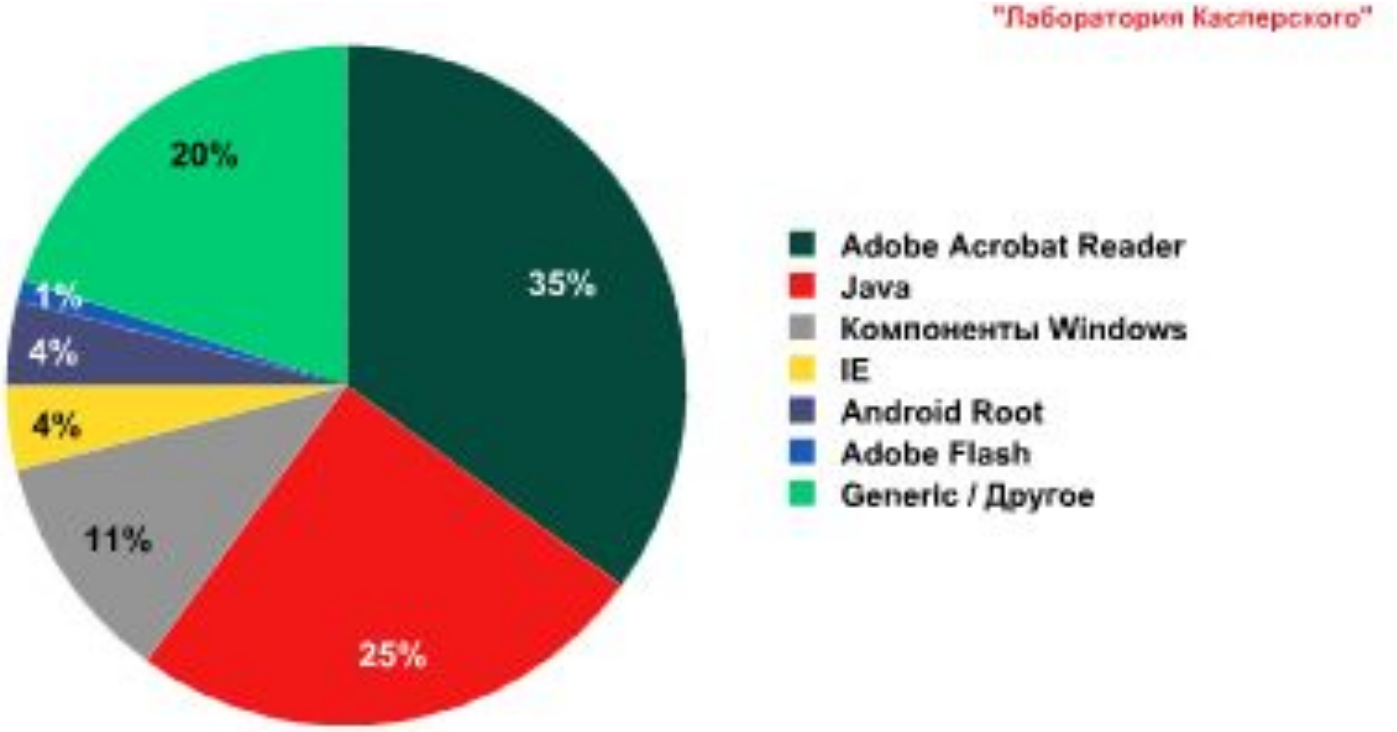
1 место – сайты с видеоконтентом (на пятом месте в 2010 году)

2 место – поисковые системы

3 место – социальные сети

Динамика развития информационных угроз

Уязвимые продукты



1 место – продукты ADOBE

2 место – JAVA

3 место – Microsoft

Патчи и легальные обновления!

Динамика развития информационных угроз

Уязвимые ОС

Массовые заражения – известные уязвимости

Zero day – для целевых атак

Динамика развития информационных угроз

Локальные инциденты

В 2011 году зафиксировано

2,3 миллиарда

локальных инцидентов!

Динамика развития информационных угроз

Картина мира

Веб-угрозы

Место	Страна	% уникальных пользователей*
1	Россия	55,9
2	Оман	54,8
3	США	50,1
4	Армения	49,6
5	Белоруссия	48,7
6	Азербайджан	47,5
7	Казахстан	47
8	Ирак	45,4
9	Украина	45,1
10	Гвинея-Бисау	45,1
11	Малайзия	44,4
12	Шри-Ланка	44,2
13	Саудовская Аравия	43,9
14	Индия	43,8
15	Судан	43,5
16	Великобритания	43,2
17	Таджикистан	43,1
18	Катар	42,4
19	Кувейт	42,3
20	Канада	42,1

Динамика развития информационных угроз

Картина мира

Локальные угрозы

Место	Страна	%
1	Судан	94,6%
2	Бангладеш	92,6%
3	Ирак	81,0%
4	Танзания	80,8%
5	Ангола	79,4%
6	Руанда	78,5%
7	Индия	77,5%
8	Непал	77,1%
9	Уганда	75,5%
10	Шри-Ланка	74,6%
11	Оман	74,3%
12	Малави	73,9%
13	Индонезия	73,6%
14	Афганистан	73,6%
15	Монголия	72,9%
16	Нигерия	71,9%
17	Мавритания	71,8%
18	Мальдивы	71,7%
19	Иран	71,5%
20	Эфиопия	70,7%

Динамика развития информационных угроз

Картина мира

Самые безопасные страны

Место	Страна*	%
1	Дания	20,6
2	Япония	21,1
3	Германия	25,3
4	Финляндия	26,3
5	Чехия	27
6	Швейцария	27,6
7	Люксембург	27,9
8	Австрия	28,4
9	Швеция	28,8
10	Норвегия	29,5
11	Нидерланды	29,7
12	Бельгия	32,3
13	Словения	32,7
14	Новая Зеландия	34,7

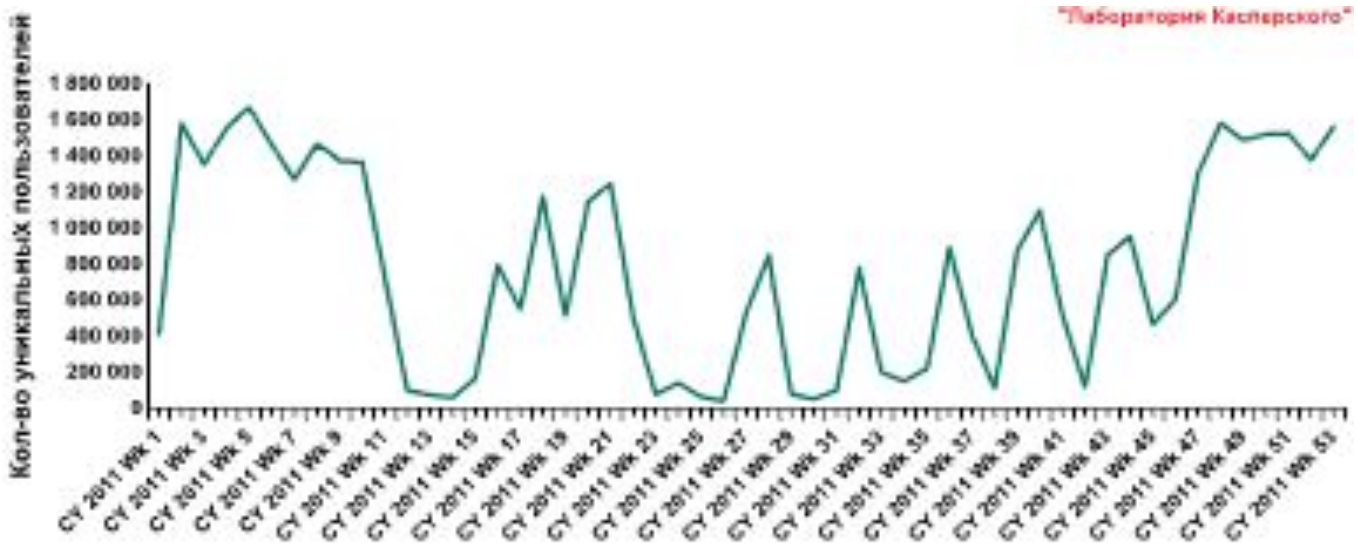
Динамика развития информационных угроз

Сетевые атаки

В 2011 году мы отразили 2 656 409 660 сетевых атак

(в прошлом году их было в 2 раза меньше)

Лидер рейтинга атак – червь Slammer



KASPERSKY lab

Динамика развития информационных угроз

2011 год. Тенденции

Тенденции

Увеличение атак с целью похищения ПД на крупные корпорации

Репутация под угрозой: Значительное количество инцидентов взломов БД
Sony, Honda, Fox News, Citibank

Наболее крупная утечка: взлом Sony: PlayStation, Qriocity, Sony Online Entertainment
Данные до 77 миллионов (!) пользователей сервисов PSN и Qriocity.

Прямой вред репутации
- сервисы Sony были недоступны по всему миру в течение 2-3 недель
- количество возвратов и обменов приставок Sony возросло в разы

«Хактивисты»
«хактивизм» — взлом или вывод из строя систем государства в знак протеста
новая группировка LulzSec: за 50 дней: взлом множества систем и ПД десятков тысяч пользователей - Sony, EA, AOL, сенат США, ЦРУ

Системным администраторам крупных компаний и государственных организаций необходимо провести тестирование своих систем, в противном случае следующая волна «хактивизма» может добраться и до них.

Тенденции

Атака на корпорацию Mitsubishi

- началась в середине сентября, готовилась в мюле-августе
- было заражено около 80 компьютеров и серверов заводов Mitsubishi
- получение и открытие PDF-файла - эксплойт уязвимости в Adobe Reader
- установка вредоносного модуля, открывающего полный удаленный доступ к системе.
- сбор и рассылка наружу интересующей информации

Тенденции

Тенденции

Тенденции

Важные цифры и факты. 2011 год

Южная Корея

- кража хакерами данных 35 миллионов пользователей социальной сети CyWorld.
- взлом серверов SK Telecom, владеющей поисковой системой Nibu и социальной сетью CyWorld.
- Всего в Республике Корея - 49 миллионов человек
- в руках злоумышленников - данные (имена, фамилии, почтовые адреса, телефоны) 3/4 населения
- Изменение политики анонимности в Интернет

Тенденции.Падение BIOS

Rootkit.Win32.Mybios.a – злобный концепт по следам Win.CIH

Основные детали
- рассчитан на заражение BIOS производства компании Award
- имеет, скорее всего, китайское происхождение
- код недоделан и содержит отладочную информацию
- стартует из BIOS после включения компьютера и может контролировать инициализацию АО и ОС
- Код, внедряемый в BIOS, восстанавливает заражение MBR
- зараженная загрузочная запись - в самом модуле ISA ROM
- компьютер останется зараженным даже в случае излечения MBR.

Трудности:
- неунифицированный формат BIOS
- алгоритм прошивки в ROM.

Еще в 1998 году вирус CIH мог портить BIOS, в результате чего становилась невозможной загрузка компьютера, но контролировать систему и передавать себе управление он не умел.

Тенденции. Проблемы с сертификатами

15 марта 2011 года - взломаны учетные записи Comodo
(защитные программные продукты и SSL-сертификаты)

Результат - создание девяти поддельных цифровых сертификатов для веб-сайтов (mail.google.com, login.yahoo.com, addons.mozilla.com и login.skype.com)

17 июня 2011 года – взломаны компьютеры сертификационного центра DigiNotar
Результат - сгенерированы более 300 поддельных сертификатов.

Потеря доверия к сертификатам и цифровым подписям

Тенденции. Кибервойны

В июне 2010 г. - обнаружен любопытный образец вредоносного ПО
Его драйверы были подписаны ворованными сертификатами

Созданный теми же людьми, что и Stuxnet, Duqu был классифицирован в августе 2011 года венгерской исследовательской лабораторией CrySyS.

- проникает на компьютер с помощью вредоносных документов Microsoft Word
- ставятся совершенно иные задачи, чем те, ради которых был создан Stuxnet.

- инструментарий для проведения атак, позволяющий взломать систему и затем систематически выкачивать оттуда информацию.
- возможность загружать на компьютер-жертву новые модули и исполнять их «на лету»

Duqu и Stuxnet – это новейшие средства для ведения кибервойн.

Мы входим в эпоху холодной кибервойны, в которой сверхдержавы борются друг с другом без сдерживающих факторов, присущих реальной войне.

Тенденции

Увеличение количества вредоносных программ для Android

В августе 2010 года - Trojan-SMS.AndroidOS.FakePlayer.a
Менее чем через год - вредоносные программы для Android - самые популярные
В III квартале 2011 года на долю Android- более 40% всего зарегистрированного вредоносного мобильного ПО.
В ноябре 2011 года - за месяц мы обнаружили более 1000 зловредов для Android!
- бурный рост спроса на саму ОС
- свободный доступ к документации = облегчение жизни злоумышленников
- слабые процесс проверки на android market

Вредоносное ПО для Mac OS
MacDefender, MacSecurity, MacProtector или MacGuard - май 2011 года
Популярность за счет черной поисковой оптимизации.
Загружают программы, затем платят за «полную версию» (40-140$)

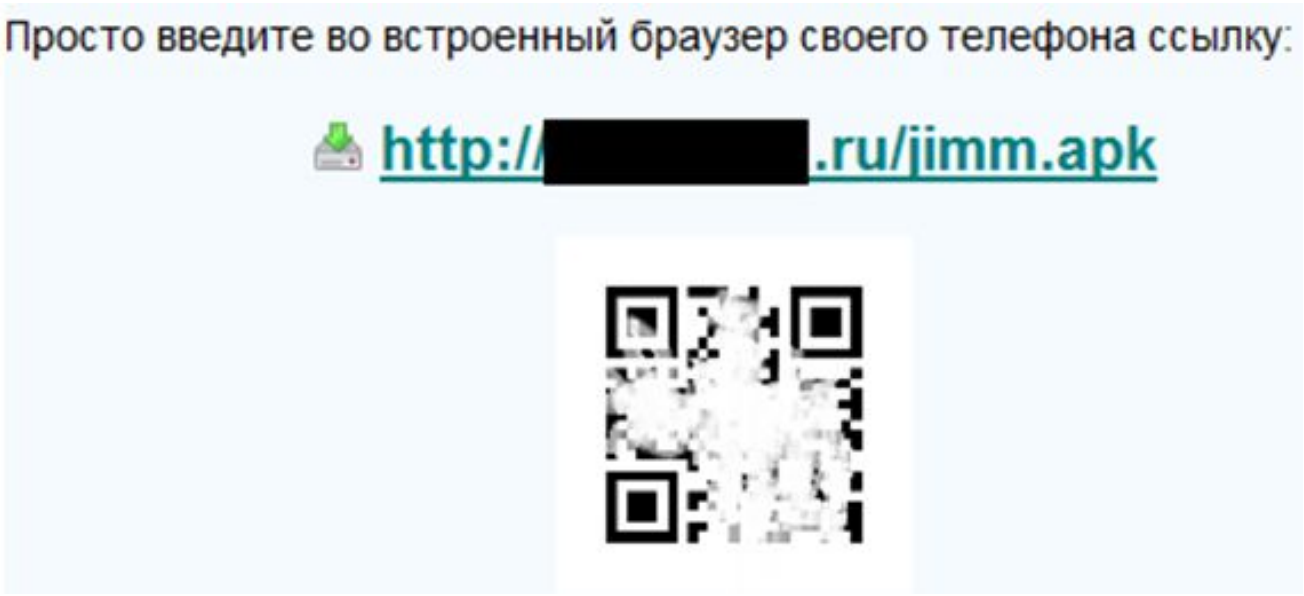
Троянцы семейства DNSChanger. (впервые – 2007 год)
Замена адреса DNS-серверов
Заход на поддельные сайты
Атаки man-in-the-middle.

Вредоносное ПО для Mac OS – это реальность!

Тенденции

Наступление мобильных угроз

Атаки с помощью QR-кодов



Прогнозы

Что нас ждет в 2012 году:

Кибероружие типа Stuxnet будет использоваться в единичных случаях.
Простые средства – «закладки», «логические бомбы» и прочее, — нацеленные на уничтожение данных в нужный момент - каждый день!

Таргетированных атак станет больше, спектр компаний и отраслей экономики, которые станут объектами атак, расширится.

В 2012 году все усилия злоумышленников – на Goggle Android. Мы ожидаем роста числа атак с использованием уязвимостей, а также появление первых мобильных Drive-by атак. Выростет число загрузок вредоносных программ в официальные магазины приложений, в первую очередь на Android Market. Мобильный шпионаж – кража данных с мобильных телефонов и слежка за объектом при помощи его телефона и геолокационных сервисов – станет широко распространенным явлением.

В 2012 году атаки на системы онлайн-банкинга возрастут.
Под ударом - Юго-Восточная Азия, Китай и страны Восточной Африки.

Множественные атаки на различные государственные и коммерческие структуры по всему миру продолжатся. При этом хактивизм может быть использован и в целях сокрытия других атак.

Как бороться?

Как вычислить слабые места

в системе безопасности государства и бизнеса?

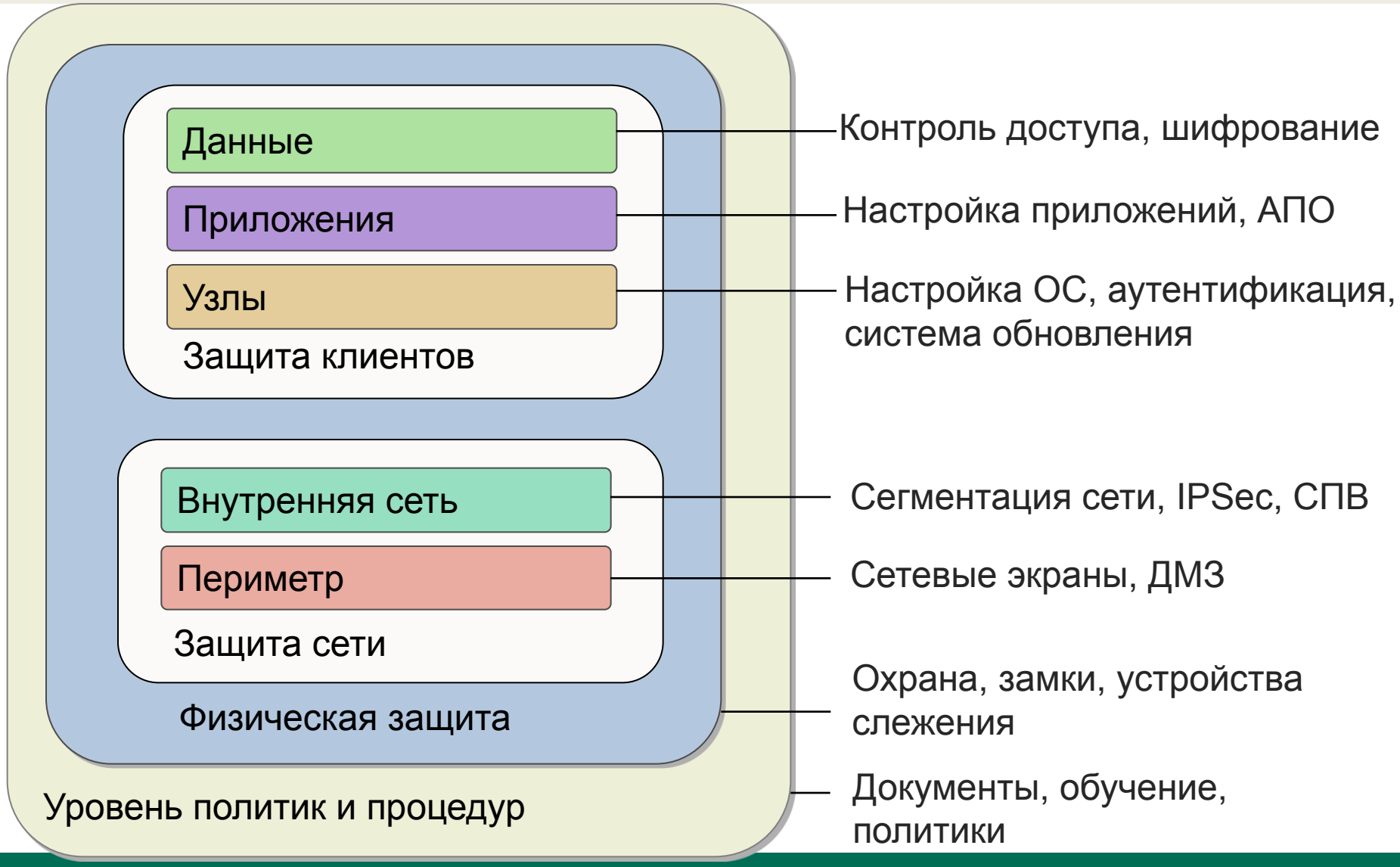
Что делать на переднем краю борьбы с информационными угрозами?

Как наносить превентивные удары?

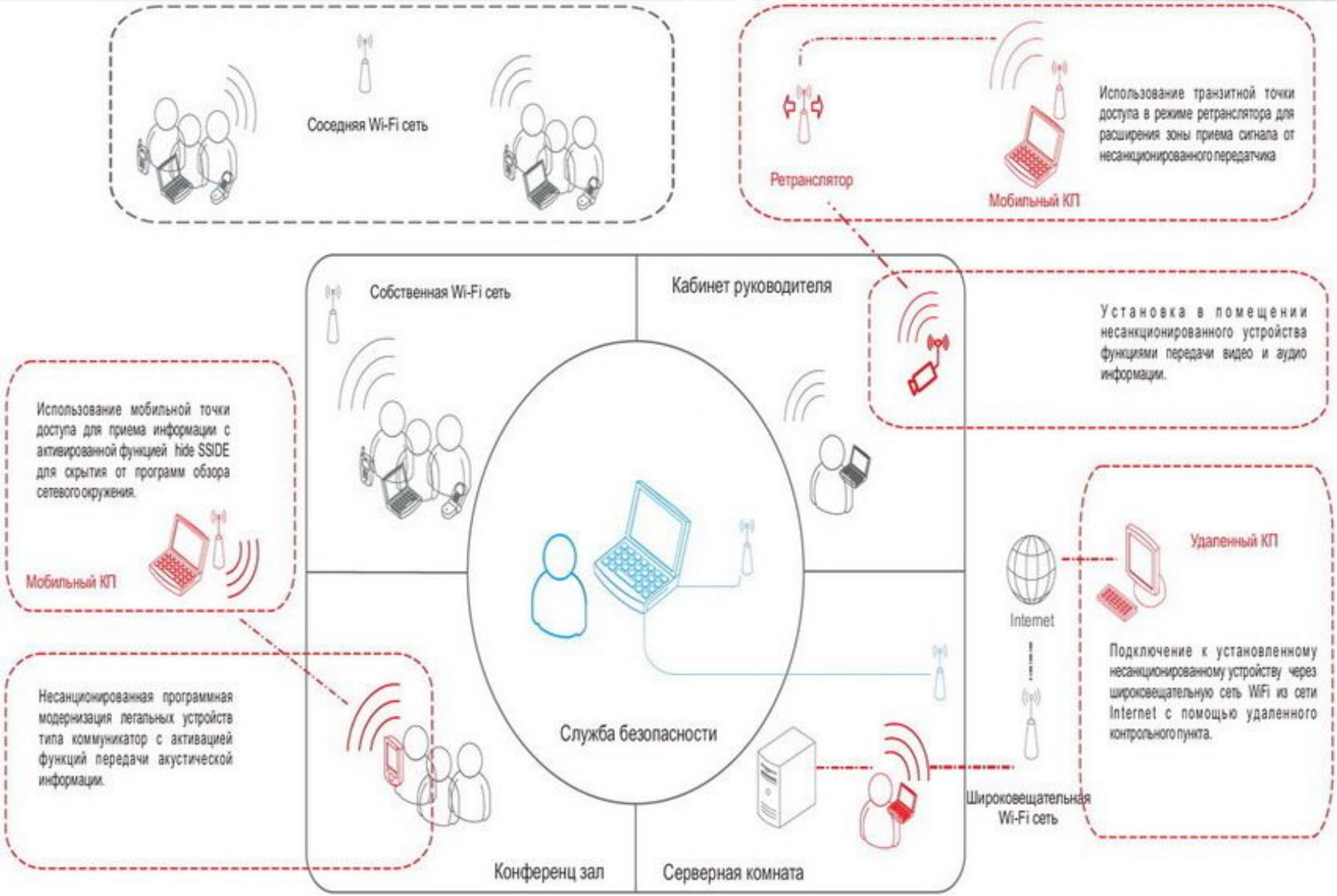
Стратегия защиты

Модель угроз
Культура работы с информацией
Политики безопасности
Физическая защита носителей
ПО для защиты информации и носителей
Дополнительные сервисы и услуги
Обмен информацией между пользователями

Модель многоуровневой антивирусной защиты



Модель угроз

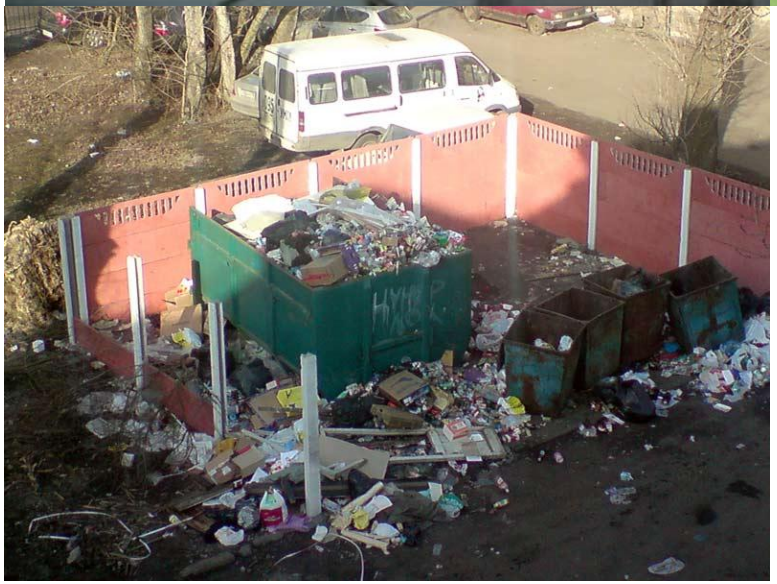


Культура работы с информацией

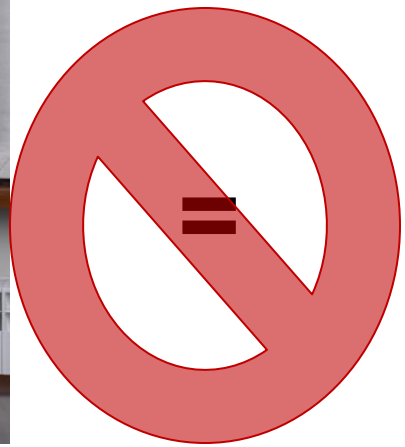
За любую бумажку с моего стола бандит полжизни отдаст!

Г.Жеглов, оперативный работник МУРа

Культура работы с информацией



Политики безопасности



Физическая защита носителей

Как предупредить действия инсайдеров

Аудит рисков ИТ-безопасности

Для компаний крайне сложно определить правильный баланс между доверием к своим сотрудниками и защитой от них же.
Компания должна ограждать себя от внутренних взломов наравне со внешними посягательствами путём следования принципам управления информационными рисками:

- оценить имеющуюся инфраструктуру
- определить критические информационные активы;
- установить текущие возможные угрозы и уязвимости
- оценить возможные денежные убытки вследствие утечки;
- выработать стратегию управления, продумать план немедленного реагирования.

Важно помнить, что избежать риска полностью нельзя.
Уменьшение риска означает нахождение золотой середины между безопасной работой компании и эффективностью бизнеса.

Как предупредить действия инсайдеров

Обучайте ваших сотрудников основам информационной безопасности

В компании должна присутствовать и развиваться культура обучения сотрудников основам информационной безопасности.

- что такое политики, процедуры
- зачем их надо соблюдать при работе
- какие средства защиты используются в сети.

Первая линия защиты от инсайдеров — это информированные сотрудники.
Разграничивайте должностные обязанности и привилегии доступа к данным

Если все сотрудники компании достаточно хорошо обучены принципам безопасности, то:
- ответственность за критические функции распределена между сотрудниками,
- эффективное разграничение бизнес-обязанностей и привилегий при работе с информацией
- максимальное количество процедур должно быть автоматизировано

Тогда:
- каждый работает только с теми документами, с которыми должен
- вероятность сговора между людьми с целью кражи ценных сведений резко снижается.

Как предупредить действия инсайдеров

Строгие политики управления учетными записями и паролями
Если учетные записи в компьютерной сети будут скомпрометированы, инсайдер получит в свои руки все инструменты подмены своих действий и сможет украсть данные

Усиление аутентификации и авторизации в сетях
Пользователи, работающие с важными данными, должны пройти аутентификацию и авторизацию при доступе к информационным ресурсам.

Деактивация несуществующих пользователей
Когда сотрудник увольняется из организации, необходимо внимательно следовать установленным процедурам увольнения и закрывать вовремя доступ ко всем информационным ресурсам

Мониторинг и сбор логов действий сотрудников в режиме реального времени
Наряду с доверием к сотрудникам не пренебрегайте мониторингом подозрительной и опасной активности, которая может иногда возникать на рабочих местах пользователей
- сильно увеличился внутренний сетевой трафик
- возросло количество запросов к корпоративной базе данных
- сильно увеличился расход тонера или бумаги.

Кроме того

- Активно защищаться от вредоносного кода хорошими антивирусными продуктами
- Использовать защиту от удаленных атак и попыток взлома.
- Внедрять резервное копирование и процедуры восстановления данных. - -

- Осуществлять контентную фильтрацию исходящего сетевого трафика.
Электронная почта, быстрые сообщения ICQ, веб- почта, постинги на форумы, блоги и другая интернет- активность должна проверяться на предмет утечек данных.
- Установить политики работы с периферийными, сменными и мобильными устройствами, на которые можно записать и унести конфиденциальный документ (FDD, CD/DVD RW, Cart Reader), присоединяемых по различным шинам (USB и PCMCIA).
- не забыть и беспроводные сети (IrDA, Bluetooth, WiFi).

- Проверять поток документов, отсылаемых на печать, чтобы предотвратить кражу документов в твердой копии.
- Фильтровать запросы к базам данных на наличие в них опасных, извлекающих секретные сведения, запросы.
- Шифровать критическую информацию на блочных устройствах и на ноутбуках.

DDOS-атаки и возможности защиты

KASPERSKY lab

Недостатки типовых методов защиты

Межсетевые экраны

Не спасают от атаки на исчерпание полосы пропускания канала.

Маршрутизация в «черные дыры»

Только помогают хакеру достичь своей цели.

Системы IDS|IPS

Не спасают от атаки на исчерпание полосы пропускания канала.

бессильны против 99% DDoS атак, которые не используют уязвимости.

Оптимизация настроек ресурсов

Правильная настройка сервера равносильна 200-300% запасы его ресурсов, что абсолютно несущественно, ибо для отражения серьезной атаки, зачастую требуется не менее 1000 процентов «запаса».

Многократное резервирование

Кластеризация, распределение ресурсов, аренда производительных каналов связи и т.п.- слишком затратны. Расходы на увеличение мощности атаки на 5-6 **порядков!!** меньше, чем расходы на такую защиту.

Общая концепция противодействия

- Информированности о угрозе, включающая
  - Информированность о типичных схемах и целях использования того или иного инструментария
  - информированность специалистов по безопасности о самой возможности что-то противопоставить злоумышленнику;
  - информированности о порядке действий в случае тех или иных инцидентов.
- Технические средства защиты
- Правовое противодействие злоумышленникам

Критерии фильтрации

Статистические

- Основа – вычисленные параметры поведения типового пользователя

Статические

- Черные/белые списки фильтрации

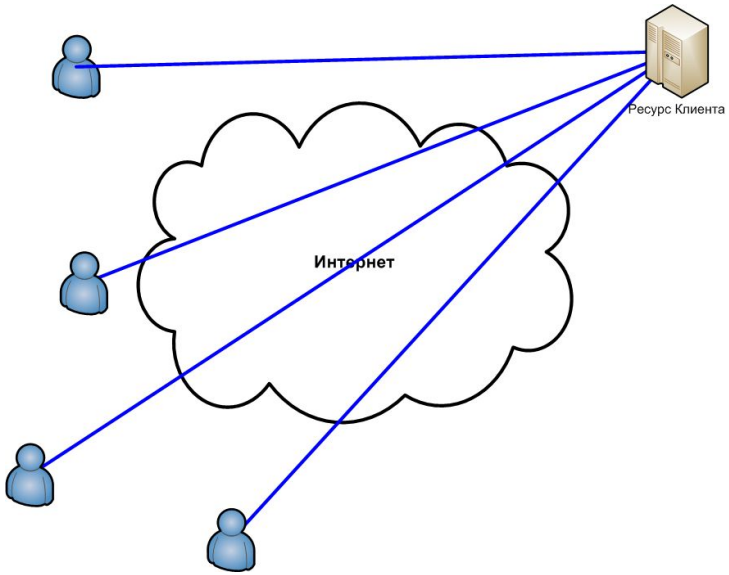
Поведенческие

- Основа – умение работать в соответствии со спецификацией протокола

Сигнатурные

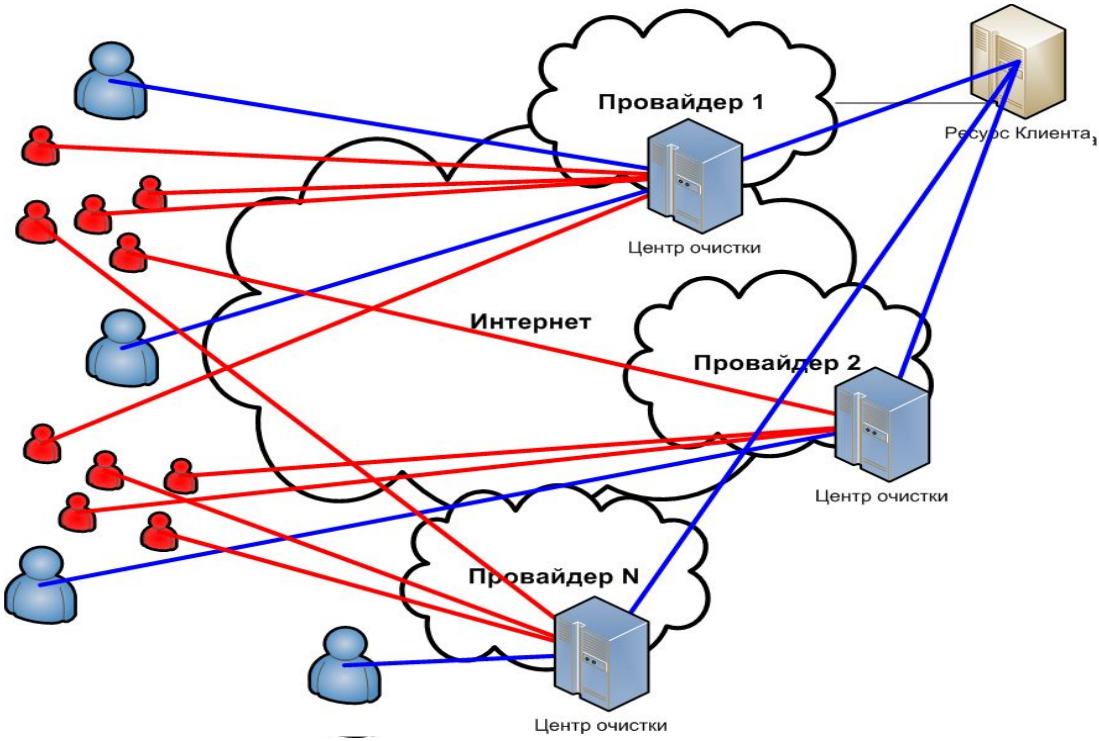
- Индивидуальные особенности Ботнета
  - Список выявленных IP адресов
  - Особенности генерируемых сетевых пакетов

Техническая идея

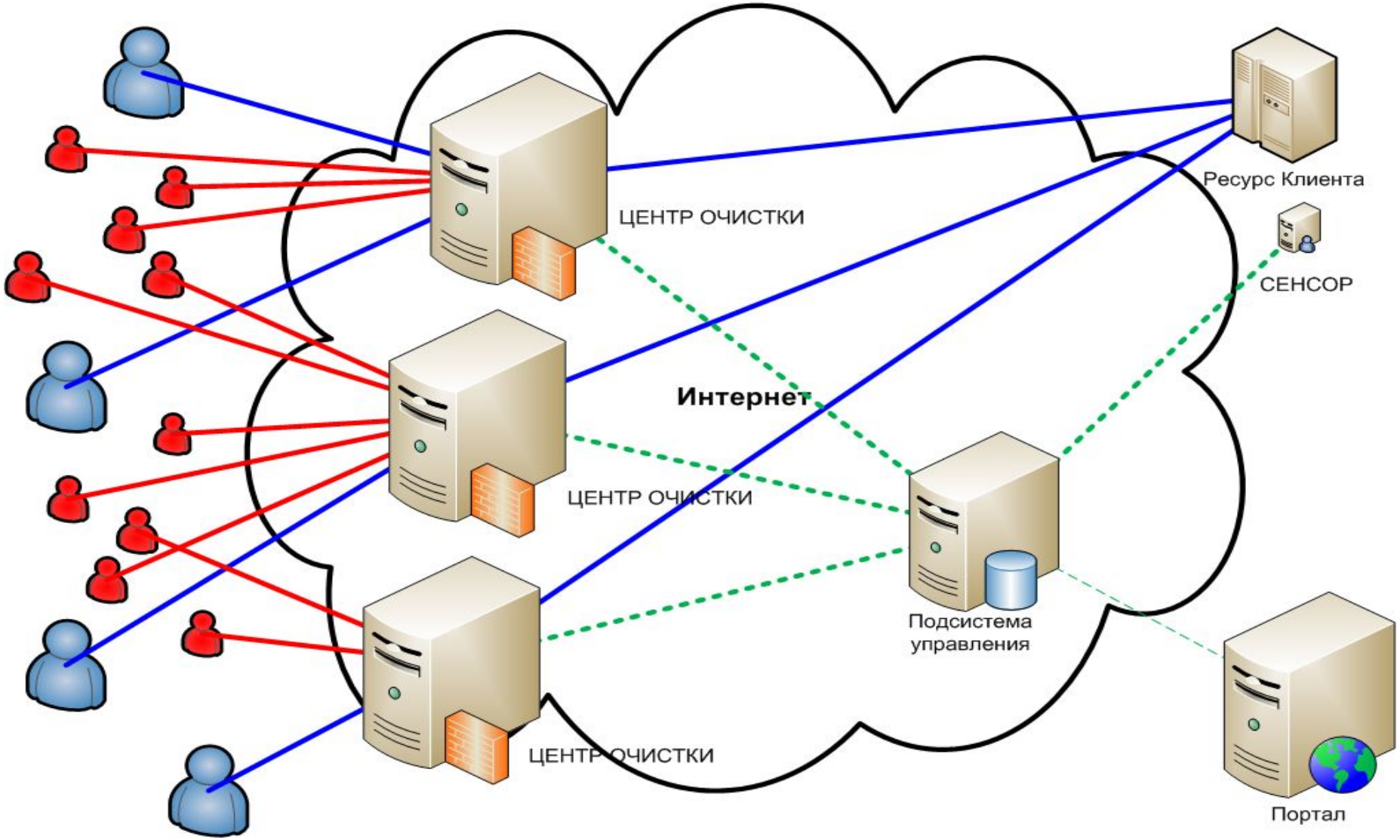


Без атаки

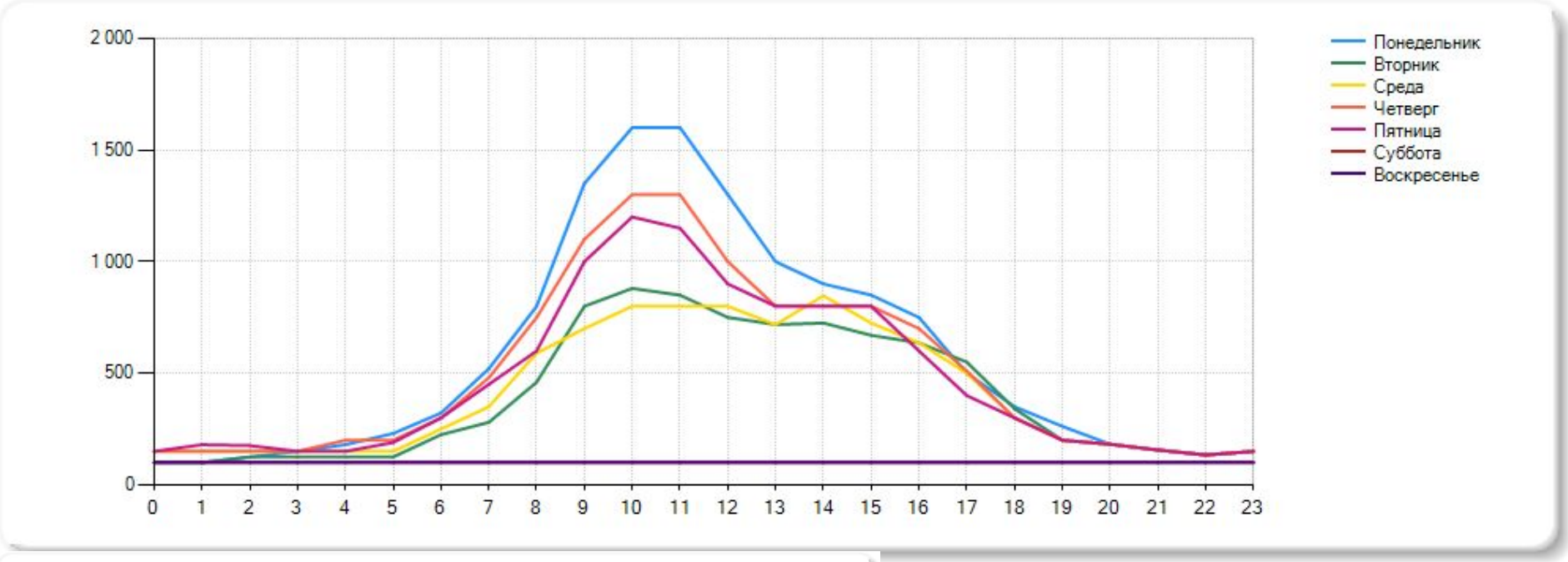
Во время атаки

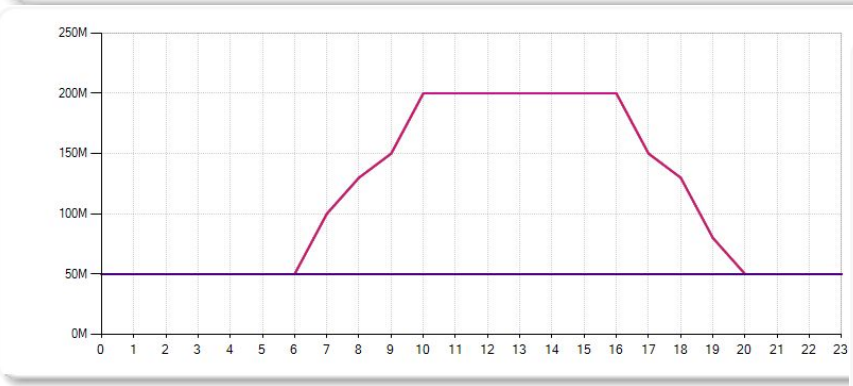


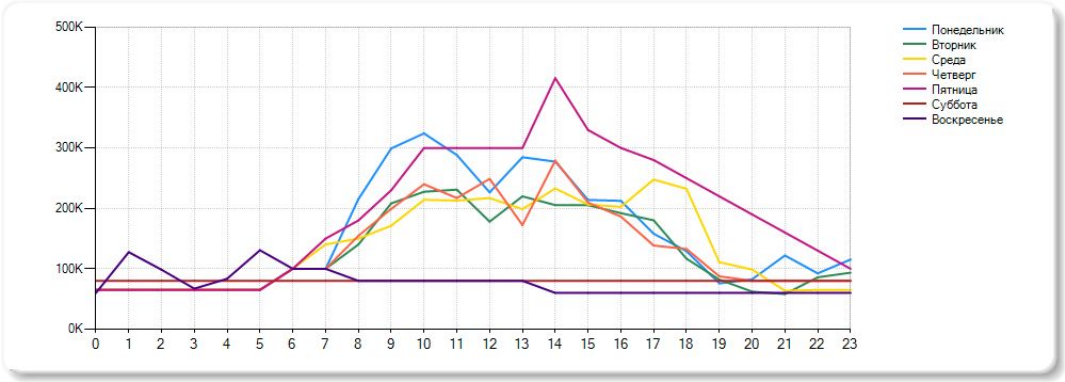
Архитектура системы



Построение профилей обнаружения







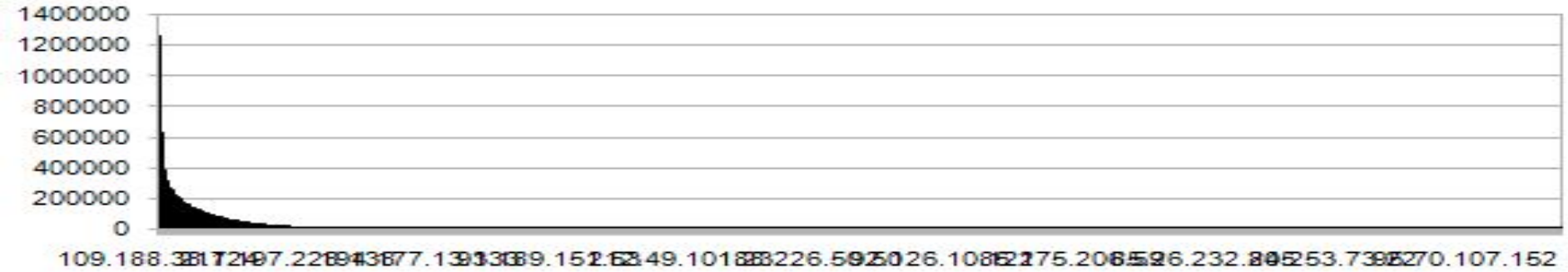
- **Работать надо вместе**
- **Невозможно защитить «пустоту»**
- **Невозможно защитить «дыру»**

Microsoft Security Bulletin MS09-048 - Critical

Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)

Published: September 08, 2009 | Updated: September 10, 2009

- **Трудно защитить того, кто не стремится к этому**



VIRUS SLA – криминологический анализ

KASPERSKY lab

KASPERSKY lab

Детки в сетке

Дети в интернете: проблема безопасности

Что есть на самом деле

Дети не рассказывают родителям о том, какие сайты посещают

33%

Родители не устанавливают никаких правил поведения в Сети

34%

Дети не обсуждают безопасность в интернете с родителями

40%

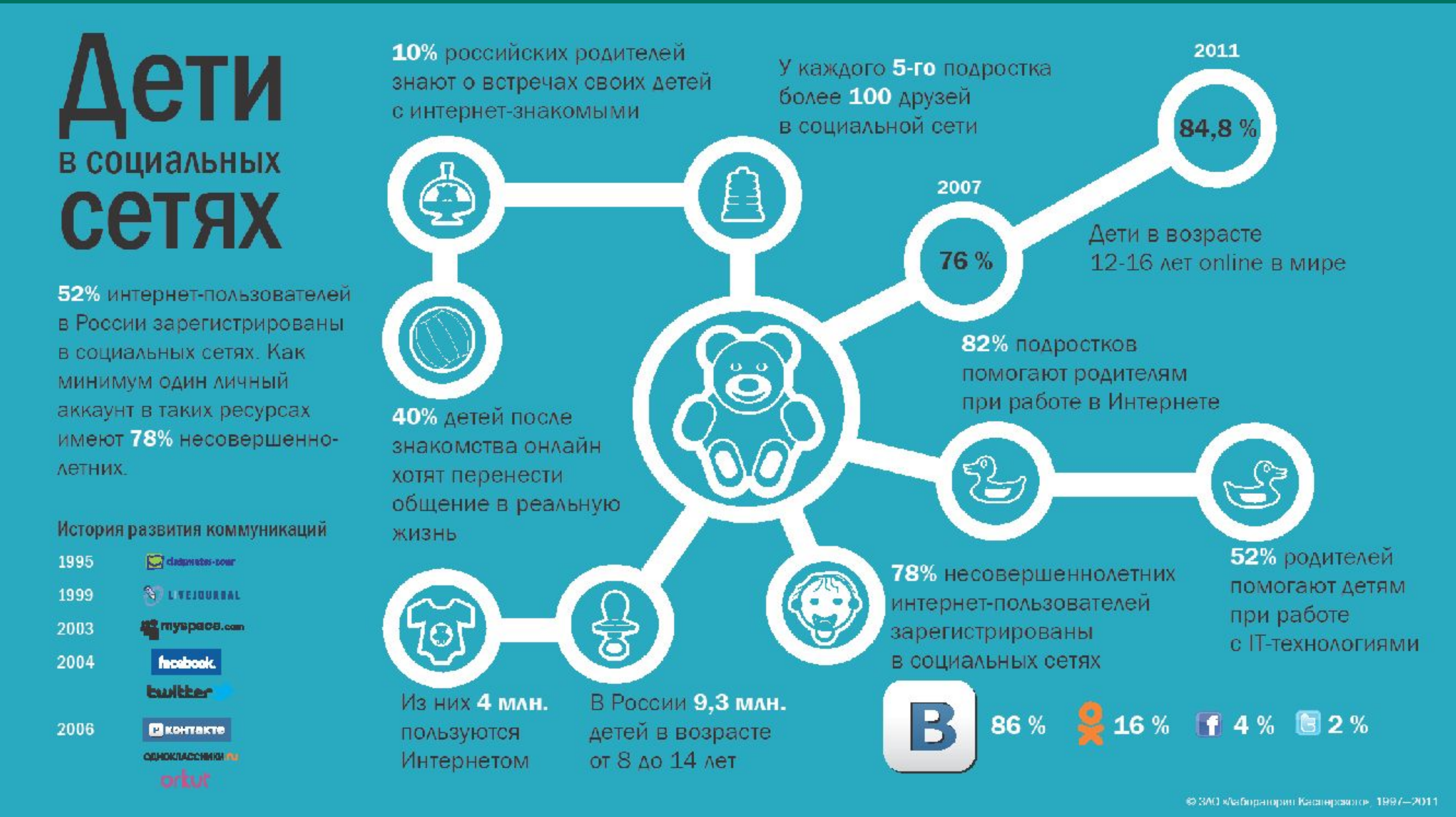
Родители не представляют, сколько времени дети тратят на Интернет

14%

Родители жалуются, что дети слишком много времени проводят в Интернете

23%

www.isafe.org



Дети
в социальных
сетях
52% интернет-пользователей в России зарегистрированы в социальных сетях. Как минимум один личный аккаунт в таких ресурсах имеют 78% несовершенно-летних.
История развития коммуникаций
1995
1999
LIVEJOURNAL
2003
myspace.com
2004
facebook.
twitter
2006
контакте
одноклассники.ru
orkut
10% российских родителей знают о встречах своих детей с интернет-знакомыми
У каждого 5-го подростка более 100 друзей в социальной сети
2011
84,8 %
2007
76 %
Дети в возрасте 12-16 лет online в мире
82% подростков помогают родителям при работе в Интернете
40% детей после знакомства онлайн хотят перенести общение в реальную жизнь
52% родителей помогают детям при работе с IT-технологиями
78% несовершеннолетних интернет-пользователей зарегистрированы в социальных сетях
Из них 4 млн. пользуются Интернетом
В России 9,3 млн. детей в возрасте от 8 до 14 лет
В
86 %
16 %
4 %
2 %
© ЗАО «Лаборатория Касперского», 1997—2011

Академия Касперского как решение проблем информационной грамотности

Kaspersky® Academy

Образовательные программы
Лаборатории Касперского

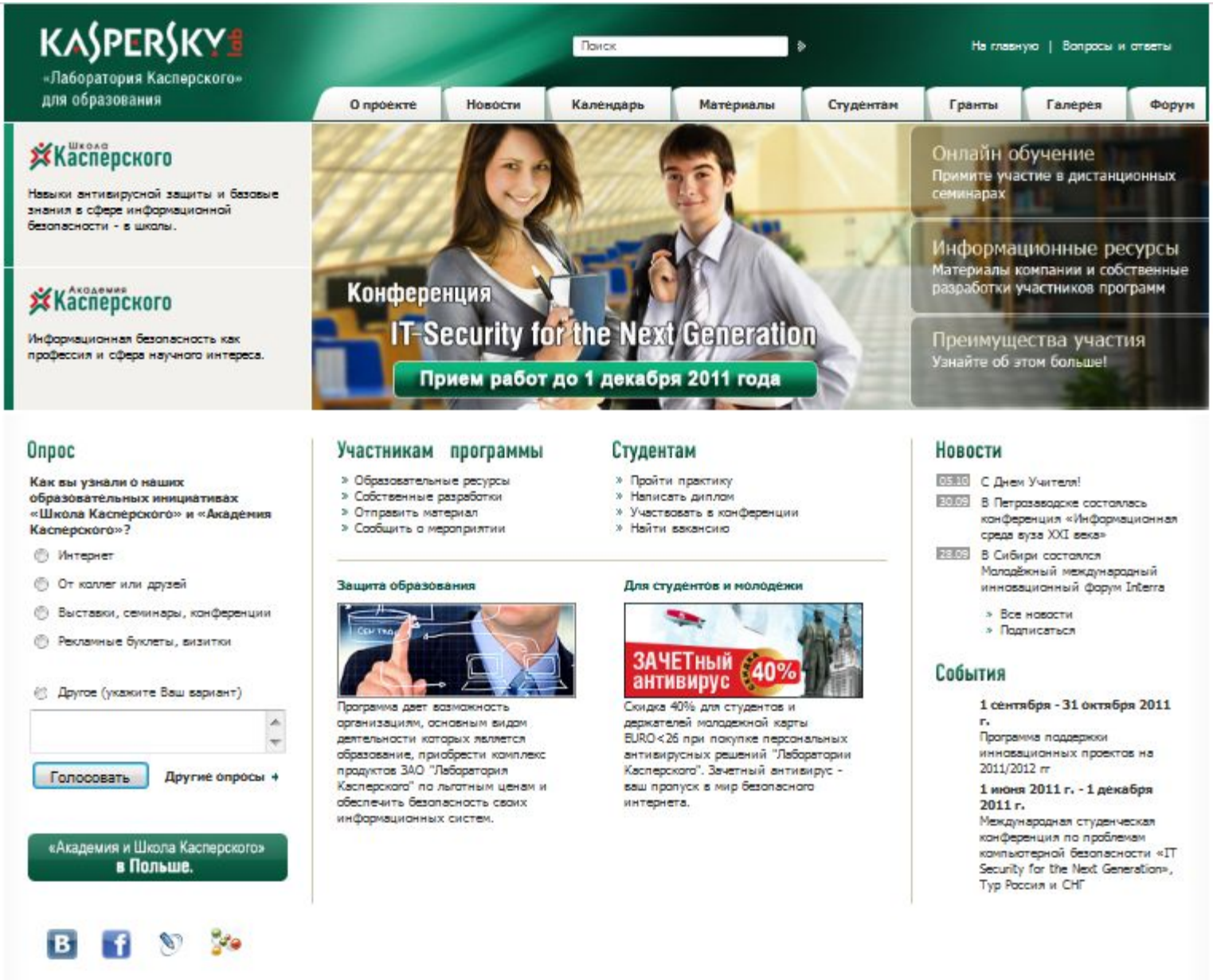
Цель программы:

Сделать доступными знания и технологии компании.

Развиваться, учиться и исследовать

ВМЕСТЕ.

www.kasperskyacademy.com

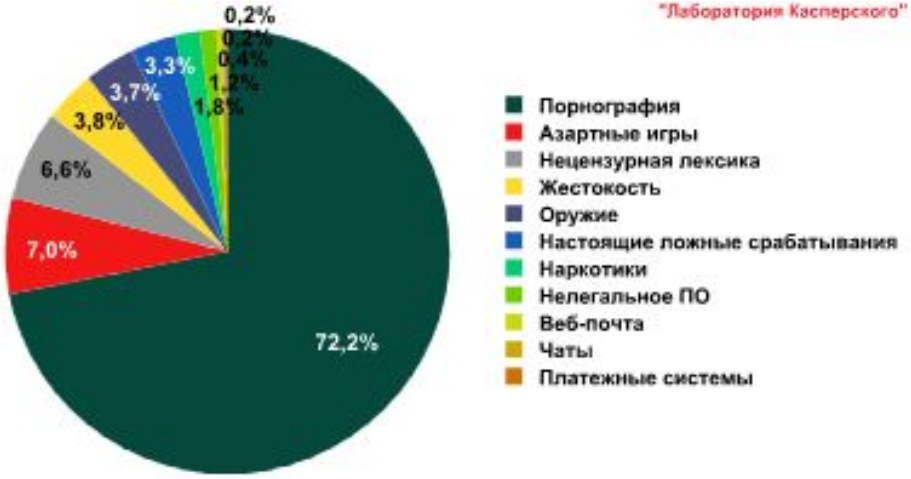


Дети и Интернет

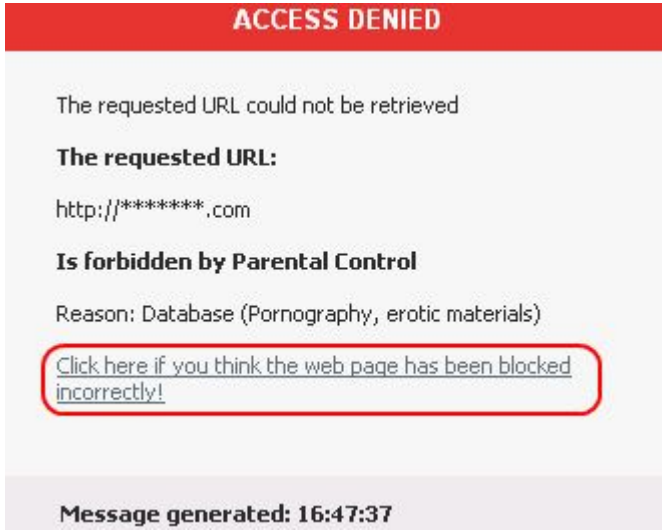
Каждый день система родительского контроля ЛК фиксирует более 4 000 000 срабатываний

80% - эротический контент и нецензурная лексика

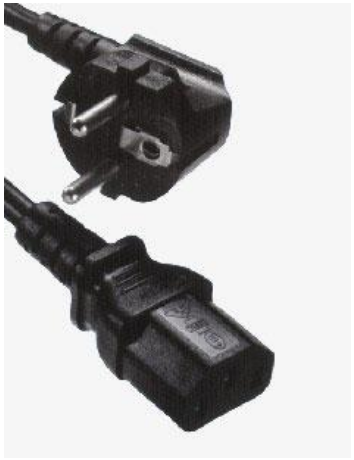
20% - наркотики, оружие, насилие



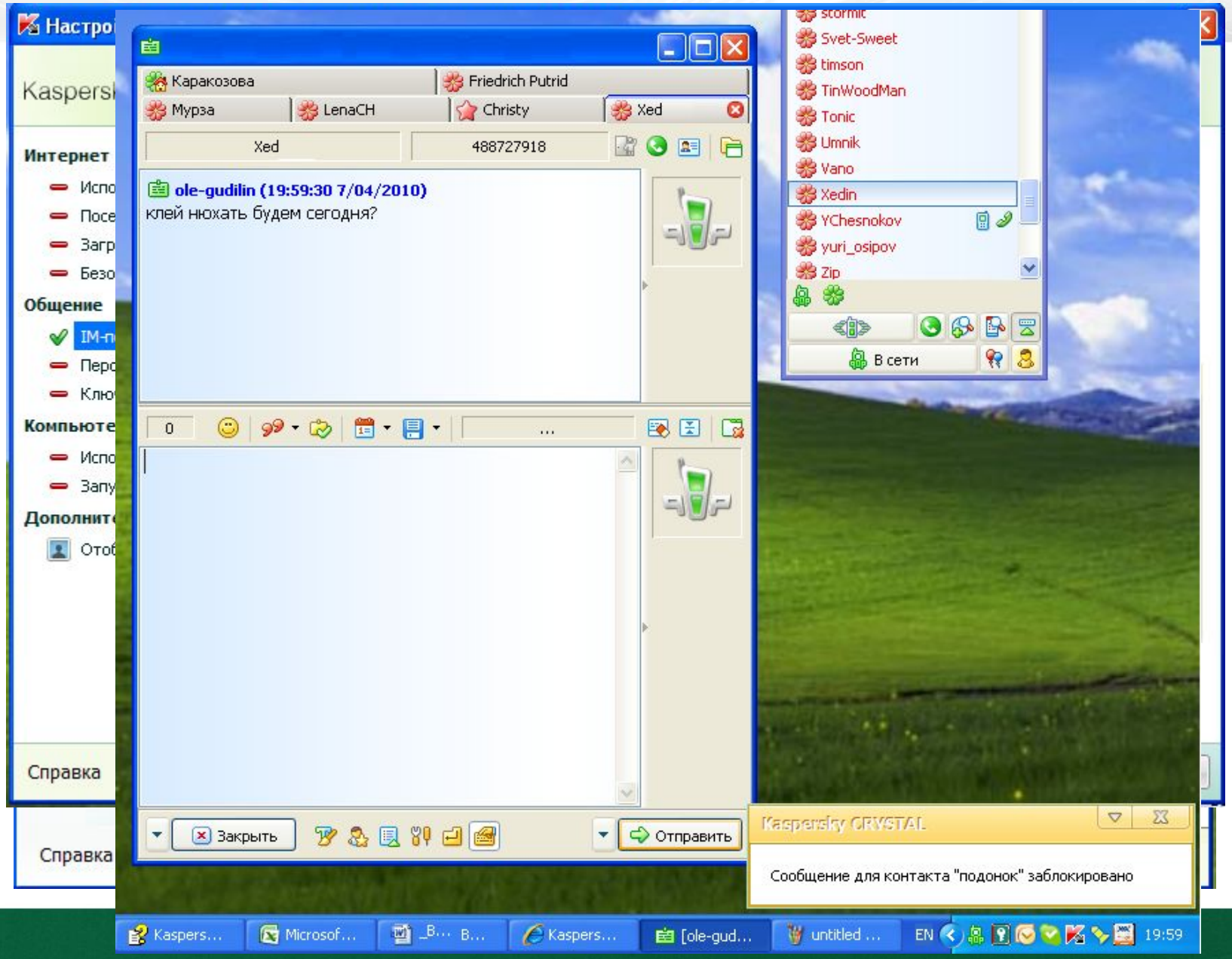
…абатывание



Какие инструменты не работают

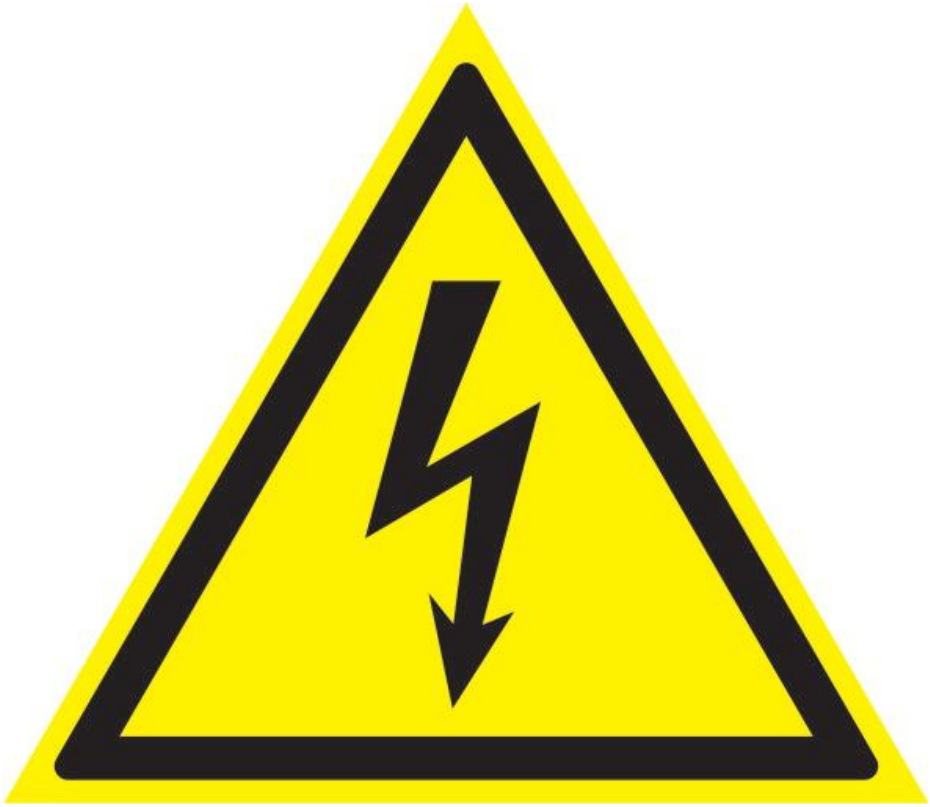


Верное решение – Kaspersky Crystal



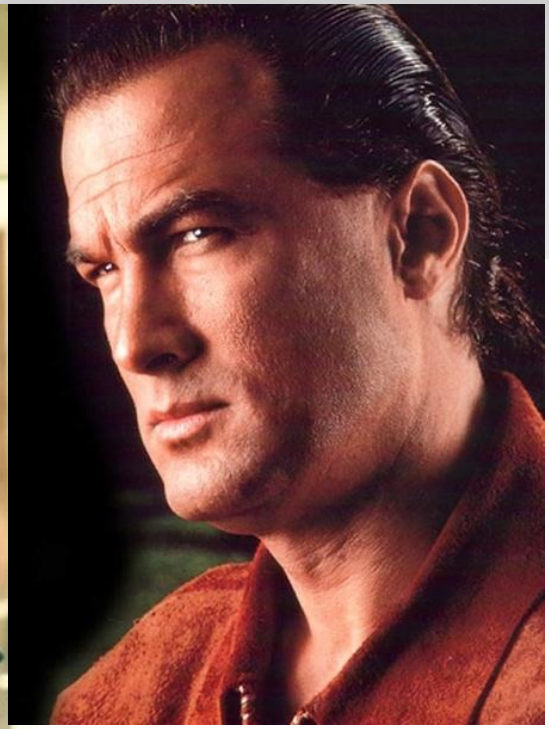
P.S.

МЫ ВСЕ В ОПАСНОСТИ




ВЫ РИСКУЕТЕ
КАЖДЫЙ ДЕНЬ
sergeydolya.livejournal.com

КОГДА ВЫ ДУМАЕТЕ ПРО IT-БЕЗОПАСНОСТЬ, ПОЛАГАЕТЕ, ОНИ ПОМОГУТ ВАМ?



НЕТ, ВАМ ПОМОГУТ ОНИ!

Спасибо!

http://www.kaspersky.ru

http://www.securelist.com/ru

KASPERSKY lab