ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Кафедра систем информационной безопасности

Информация и ее ценность

- Первый закон - Федеральный закон Российской Федерации «Об информации, информатизации и защите информации» №24-ФЗ от 20.02.95:
- информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
- №149-ФЗ "Об информации, информационных технологиях и о защите информации" от 27.07.2006
- **Доктрина информационной безопасности РФ**

УКАЗ

ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

Об утверждении Доктрины
информационной безопасности Российской Федерации

В целях обеспечения информационной безопасности Российской Федерации п о с т а н о в л я ю:

1. Утвердить прилагаемую Доктрину информационной безопасности Российской Федерации.

2. Признать утратившей силу Доктрину информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

3. Настоящий Указ вступает в силу со дня его подписания.

Президент
Российской Федерации В.Путин

Москва, Кремль
5 декабря 2016 года
№ 646

Доктрина информационной безопасности

- это система официальных взглядов на обеспечение национальной безопасности РФ в информационной сфере.
- Обеспечение и защита прав и свобод граждан в части получения и использования информации, неприкосновенность частной жизни, а также сохранение духовно-нравственных ценностей.
- Бесперебойное функционирование критической информационной инфраструктуры.
- Развитие в России отрасли ИТ и электронной промышленности.
- Доведение до российской и международной общественности достоверной информации о государственной политике РФ.
- Содействие международной информационной безопасности.

Доктрина информационной безопасности

Информационная безопасность РФ - состояние защищенности:
личности, общества и государства
от внутренних и внешних информационных угроз,

при котором обеспечивается:

- реализация конституционных прав и свобод человека и гражданина,
- достойные качество и уровень жизни граждан,
- суверенитет,
- территориальная целостность и устойчивое социально-экономическое развитие РФ,
- оборона и безопасность государства.

Доктрина информационной безопасности

ОСНОВНЫЕ УГРОЗЫ

- зарубежные страны наращивают возможности по воздействию на ИТ инфраструктуру в военных целях.
- усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских организаций.
- внедрение ИТ без увязки с ИБ повышает вероятность проявления угроз.
- специальные службы используют методы информационно-психологическое воздействия на граждан.

Доктрина информационной безопасности

ОСНОВНЫЕ УГРОЗЫ

- все больше зарубежных СМИ доносят информацию предвзято.
- Российские СМИ за рубежом подвергаются дискриминации.
- внешнее информационное воздействие размывает традиционные российские духовно-нравственные ценности (особенно у молодежи).
- террористические и экстремистские организации широко используют механизмы информационного воздействия.

Доктрина информационной безопасности

ОСНОВНЫЕ УГРОЗЫ

- возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере
- методы, способы и средства совершения компьютерных преступлений становятся все изощрённее.
- повышается сложность и количество скоординированных компьютерных атак на объекты КИИ.
- остается высоким уровень зависимости отечественной промышленности от зарубежных ИТ.

Доктрина информационной безопасности

ОСНОВНЫЕ УГРОЗЫ

- российские научные исследования в сфере ИТ являются недостаточно эффективными, ощущается недостаток кадров.
- у Российских граждан низкая осведомленность в вопросах обеспечения личной ИБ.
- отдельные государства стремятся использовать технологическое превосходство для доминирования в информационном пространстве. В том числе и в сети Интернет.

Статьи в УК РФ

- Ст. 272 УК РФ – «Неправомерный доступ к компьютерной информации». (2/7)
- Ст. 273 УК РФ – «Создание, использование и распространение вредоносных компьютерных программ» (4/7)
- Ст. 274 УК РФ – «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»(2/5)

Информация и ее ценность

- информации может иметь ценность, собственника, пользователя и владельца информационных ресурсов и, следовательно, являться объектом права.

Информация и ее ценность

- «информационная война» - особый вид отношений между государствами, при котором для разрешения существующих межгосударственных противоречий используются методы, средства и технологии силового воздействия на информационную сферу этих государств.

Информационное оружие:

- компьютерный вирус,
- программная закладка,
- цветные революции.

Основные понятия и определения

- Под безопасностью автоматизированных систем обработки информации (АСОИ) понимают их защищенность от случайного или преднамеренного вмешательства в нормальный процесс их функционирования, а также от попыток хищения, изменения или разрушения их компонентов
- Субъект доступа – это активный компонент системы (пользователь, процесс, прикладная программа и т.п.).
- Объект доступа – это пассивный компонент системы, хранящий, принимающий или передающий информацию (файл, каталог и т.п.).

Основные понятия и определения

- Санкционированный доступ к информации – это доступ, не нарушающий установленные *правила*.
- Несанкционированный доступ (НСД) к информации – доступ, нарушающий установленные правила.

Базовые свойства безопасности информации

- С точки зрения информационной безопасности выделяют следующие свойства информации:
- КОНФИДЕНЦИАЛЬНОСТЬ;
- ЦЕЛОСТНОСТЬ;
- ДОСТУПНОСТЬ.

Базовые свойства безопасности информации

- *Конфиденциальность информации* – это ее свойство быть известной только допущенным и прошедшим проверку (*авторизованным*) субъектам системы. Для остальных субъектов системы эта информация должна быть неизвестной.

Базовые свойства безопасности информации

- *Целостность информации* – ее свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий.

Базовые свойства безопасности информации

- *Доступность информации* – ее свойство быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов.

Базовые свойства безопасности информации

- *Целью злоумышленника* является реализация какого-либо рода действий, приводящих к невыполнению (нарушению) одного или нескольких из свойств конфиденциальности, целостности или доступности информации.

Базовые свойства безопасности информации

- Потенциальные возможности реализаций определенных воздействий на АСОИ, которые прямо либо косвенно могут нанести ущерб ее безопасности, называются *угрозами безопасности АСОИ*.
- *Уязвимость АСОИ* – некоторое неудачное свойство системы, которое делает возможным возникновение и реализацию угрозы.
- *Атака на компьютерную систему* – это непосредственная реализация злоумышленником угрозы безопасности.

Базовые свойства безопасности информации

- Цель системы защиты информации – противодействие угрозам безопасности в АСОИ.
- По цели воздействия выделяют три основных типа угроз безопасности АСОИ :
- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения работоспособности системы (отказы в обслуживании).

Базовые свойства безопасности информации

- *Случайные воздействия* - аварийные ситуации из-за стихийных бедствий и отключений электропитания, отказы и сбои в аппаратуре, ошибки в программном обеспечении, ошибки в работе обслуживающего персонала и пользователей и т.д.

- *Преднамеренные угрозы* связаны с целенаправленными действиями нарушителя и могут быть обусловлены разными мотивами: недовольством служащего карьерой, материальным интересом, любопытством, конкурентной борьбой и т.д.

Базовые свойства безопасности информации

- При реализации угроз безопасности злоумышленник может воспользоваться самыми различными *каналами реализации угроз* – каналами НСД, каналами утечки.

- Под *каналом утечки информации* понимают совокупность источника информации, материального носителя или среды распространения, несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя.

Базовые свойства безопасности информации

- Выделяют следующие основные каналы утечки информации:
- ЭЛЕКТРОМАГНИТНЫЙ КАНАЛ;
- ВИБРОАКУСТИЧЕСКИЙ КАНАЛ;
- ВИЗУАЛЬНЫЙ КАНАЛ;
- ИНФОРМАЦИОННЫЙ КАНАЛ.

Основные принципы обеспечения информационной безопасности

- Системности.
- Комплексности.
- Непрерывности защиты.
- Разумной достаточности.
- Гибкости управления и применения.
- Открытости алгоритмов и механизмов защиты.
- Простоты применения защитных мер и средств.

Ценность информации

- Под *ценностью информации* понимается ее свойство, характеризующее потери собственника данной информации при реализации определенной угрозы, выраженные в стоимостном, временном либо ином эквиваленте.

Меры обеспечения безопасности

- правовые (законодательные);
- морально-этические;
- организационно-административные;
- физические;
- **АППАРАТНО-ПРОГРАММНЫЕ.**

Аппаратно-программные меры

- идентификацию и аутентификацию субъектов АСОИ;
- разграничение доступа к ресурсам АСОИ;
- контроль целостности данных;
- обеспечение конфиденциальности данных;
- аудит событий, происходящих в АСОИ;
- резервирование ресурсов и компонентов АСОИ.

Политики безопасности

Дискреционная матрица

Субъект / Объект	Файл 1	Файл 2	CD-RW	Флоппи-дисковод
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Полные права

Политики безопасности

Мандатная политика

CD-RW	Конфиденциально
Флоппи-дисковод	не конфиденциально
Файл 1	секретно
Файл 2	совершенно секретно

Администратор	совершенно секретно
Пользователь 1	секретно
Гость	Не конфиденциально
Пользователь 2	конфиденциально

Идентификация и аутентификация

- Под *идентификацией* понимают присвоение пользователю некоторого уникального идентификатора, который он должен предъявить, то есть назвать себя.

- Под *аутентификацией* понимают подтверждение пользователем предъявленного идентификатора, проверка его подлинности и принадлежности именно данному пользова-телю.

Идентификация и аутентификация

- Парольные системы.
- Идентификация/аутентификация с использованием технических устройств.
- Идентификация/аутентификация с использованием индивидуальных биометрических характеристик пользователя.

Парольные системы

- перебор паролей в интерактивном режиме.
- подсмотр пароля.
- преднамеренная передача пароля его владельцем другому лицу.
- кража базы данных учетных записей.
- перехват вводимого пароля путем внедрения в КС программных закладок (клавиатурных шпионов) или перехват пароля, передаваемого по сети.
- социальная инженерия.

Парольные системы

Если алфавит: 26+26+10=62

Длина пароля **6 СИМВОЛОВ**

62^6 = 56 800 235 584 паролей

10 000 000 паролей в секунду

$62^{10}/10^7$=5 680 секунд

5 680 секунд/3600 секунд

1,5 часа

Парольные системы

Время перебора возможных вариантов паролей

Длина пароля Символы	6	8	10
Англ. больш. и мал., Цифры: 62	1,6 ч.	252 сут.	2661 г.
Англ. больш. и мал., Цифры, Спец символы: 92	16 ч.	16 лет	137743 лет

Требования к паролю

Длина не менее 9 символов, содержащих

прописные и строчные буквы
+
специальные символы
+
цифры

Простой для запоминания, но сложный для взлома пароль

В лесу родилась

@B@лесу@родилась = 96^{16}

@D@ktce@hjlbkfcm =86^{16}

$$\frac{5{,}2*10^{31}}{10^{7}} = 1{,}6 * 10^{17} \text{ лет}$$

(больше возраста вселенной)

Технические устройства идентификации и аутентификации

- идентификаторы iButton (Touch Memory);
- бесконтактные радиочастотные карты proximity;
- пластиковые карты;
- ключи e-Token.

Индивидуальные биометрические характеристики пользователя

- отпечатки пальцев;
- геометрическая форма рук;
- узор радужной оболочки и сетчатки глаз;
- форма и размеры лица;
- особенности голоса;
- биомеханические характеристики почерка;
- биомеханические характеристики «клавиатурного почерка».

Индивидуальные биометрические характеристики пользователя

Меры обеспечения безопасности

- правовые (законодательные);
- морально-этические;
- организационно-административные;
- физические;
- **АППАРАТНО-ПРОГРАММНЫЕ**.

Криптографическая защита информации

- *Криптография* представляет собой совокупность методов преобразования данных (шифрования), направленных на то, чтобы сделать эти данные бесполезными для противника.
- Эти преобразования позволяют решить проблему обеспечения конфиденциальности данных.
- Управление процессом шифрования осуществляется с помощью *ключа* шифрования.
- *Криптоанализ* - раскрытие шифра и получение открытого текста, не имея подлинного ключа шифрования.

Криптоаналитические атаки

1. Криптоаналитическая атака при наличии известного открытого текста (атака по открытому тексту).
2. Криптоаналитическая атака методом полного перебора всех возможных ключей (силовая атака, атака «в лоб», или brute-forcing).
3. Криптоаналитическая атака методом анализа частотности закрытого текста.

Криптографическая защита информации

Основной характеристикой шифра является его *криптостойкость*, которая определяет его стойкость к раскрытию с помощью методов криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

Требования к шифрам

1. Зашифрованный текст должен поддаваться чтению только при наличии секретного ключа шифрования.
2. *Закон Керхоффа* – знание алгоритма шифрования не должно влиять на надежность защиты, стойкость шифра должна определяться только секретностью ключа. Иными словами, данное требование предполагает, что весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника.
3. Единственно возможный метод раскрытия шифротекста должен заключаться в дешифровании его на секретном ключе. Единственно возможный способ нахождения ключа дешифрования должен заключаться в полном их переборе.
4. При знании криптоаналитиком шифротекста и соответствующего ему открытого текста, для нахождения ключа шифрования необходим полный перебор ключей.
5. Незначительное изменение ключа шифрования или открытого текста должно приводить к существенному изменению вида шифротекста.
6. Избыточность информации, вносимая в шифротекст за счет шифрования, должна быть незначительной.
7. Алгоритм шифрования должен допускать как программную, так и аппаратную реализацию.

Традиционные симметричные криптосистемы

В симметричных криптосистемах (криптосистемах с секретным ключом) шифрование и дешифрование информации осуществляется на одном ключе, являющемся секретным.

Традиционные симметричные криптосистемы

- Шифры замены.
- Шифры перестановки.
- Шифры гаммирования.

Традиционные симметричные криптосистемы

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее оговоренной схемой замены.

Традиционные симметричные криптосистемы

Шифрование заменой

Шифрование методом Цезаря (около 50 г. до н.э).

При шифровании каждая буква заменяется на другую букву того же алфавита путем ее смещения в используемом алфавите на 3 позиции.

Пример: БАГАЖ → ДГЖГЙ

А → Г	Р → У
Б → Д	С → Ф
В → Е	Т → Х
Г → Ж	У → Ц
Д → З	Ф → Ч
Е → И	Х → Ш
Ж → Й	Ц → Щ
З → К	Ч → Ь
И → Л	Ш → Ы
Й → М	Щ → Ъ
К → Н	Ь → Э
Л → О	Ы → Ю
М → П	Ъ → Я
Н → Р	Э → А
О → С	Ю → Б

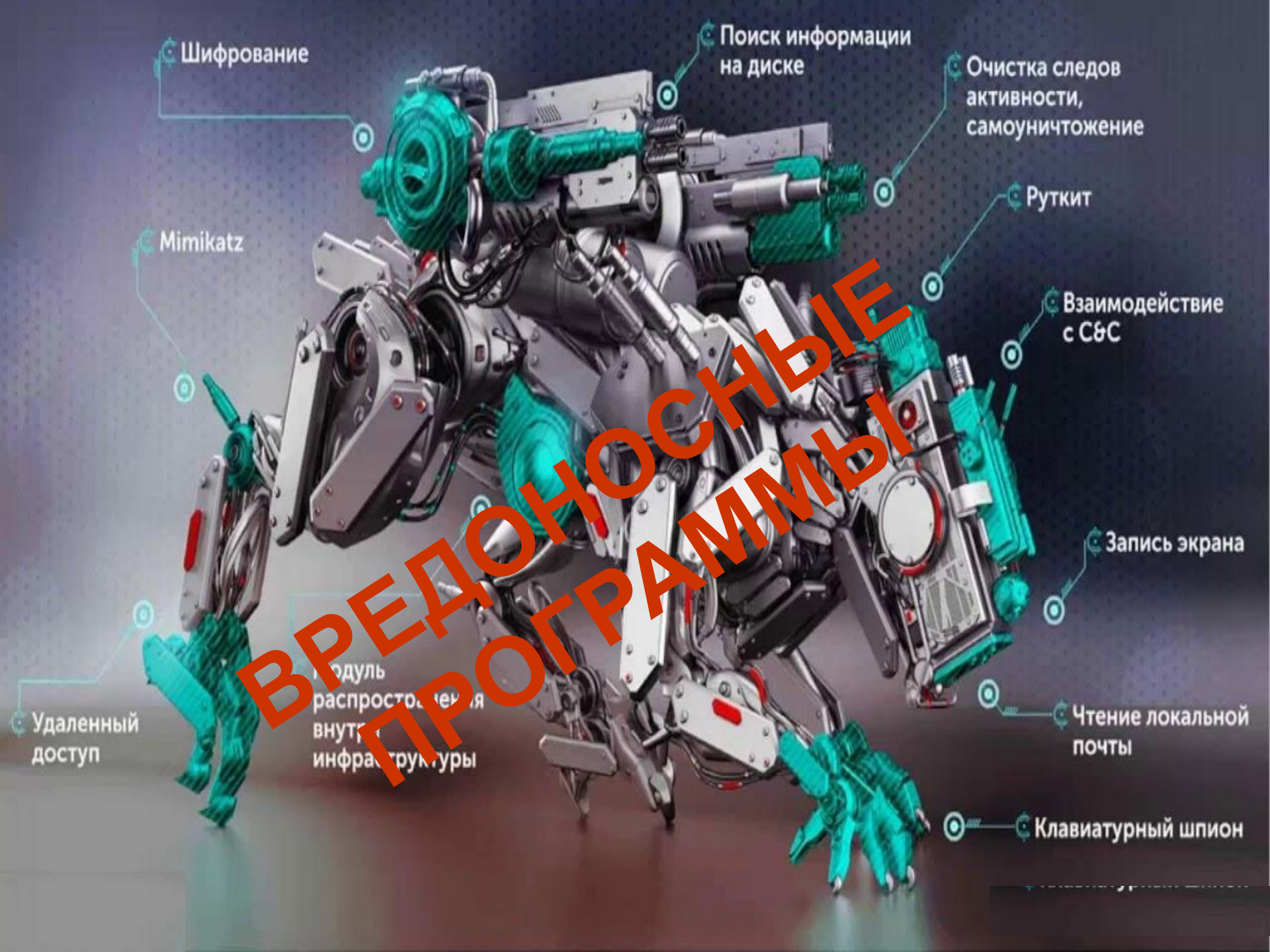
Традиционные симметричные криптосистемы

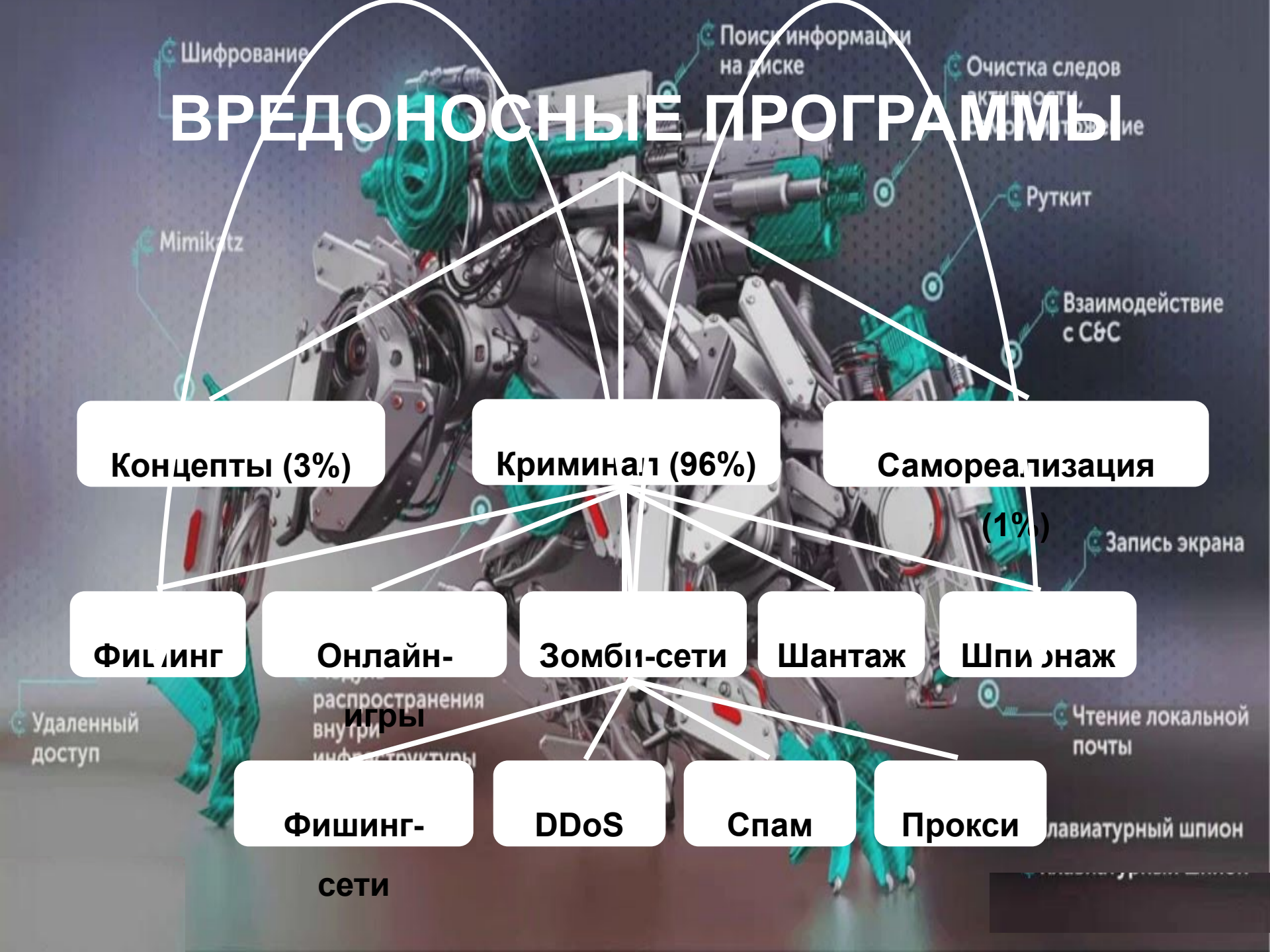
Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста.

«Простая перестановка»

Ключ: 3142. Текст разбивается на блоки = длине ключа. Ключ определяет порядок следования символов.

П	**Р**	**И**	**Е**	**З**	**Ж**	**А**	**Ю**	**Д**	**Н**	**Е**	**М**
3	**1**	**4**	**2**	**3**	**1**	**4**	**2**	**3**	**1**	**4**	**2**
И	**П**	**Е**	**Р**	**А**	**З**	**Ю**	**Ж**	**Е**	**Д**	**М**	**Н**


Шифрование
Поиск информации на диске
Очистка следов активности, самоуничтожение
Руткит
Mimikatz
Взаимодействие с C&C
ВРЕДОНОСНЫЕ ПРОГРАММЫ
Запись экрана
Удаленный доступ
Чтение локальной почты
Клавиатурный шпион



ВРЕДОНОСНЫЕ ПРОГРАММЫ

- Концепты (3%)
- Криминал (96%)
  - Фишинг
  - Онлайн-игры
  - Зомби-сети
    - Фишинг-сети
    - DDoS
    - Спам
    - Прокси
  - Шантаж
  - Шпионаж
- Самореализация (1%)

ВРЕДОНОСНАЯ ПРОГРАММА

- Программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

- (компьютерный) вирус: Вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

/ГОСТ Р 51275-2006

Вирусы

- Программы, которые заражают другие программы – добавляют в них свой код, чтобы получить управление при запуске зараженных файлов.
- хранятся на диске

Троянские программы (Trojans)

- Собирают информацию о пользователе и системе
- хранятся на диске
- Нужен Internet

Черви (Worms)

- «переползают» с компьютера на компьютер, используя сети и электронную почту
- не хранятся на диске
- собирают информацию о пользователе и системе

Бот

- Компьютер управляемый червем
- Боты объединены в бот-сети
- DOS-атака
- Рассылка SPAM
- В бот-сети от десятков до сотен тысяч ботов
- Бот-сетей >> 10 000

DOS-атака

- Denial Of Service – отказ в обслуживании.
- Большое количество соединений (100 и более) с атакующего компьютера к серверу. В результате чего сервер становится недоступным для других.

DDoS-атака

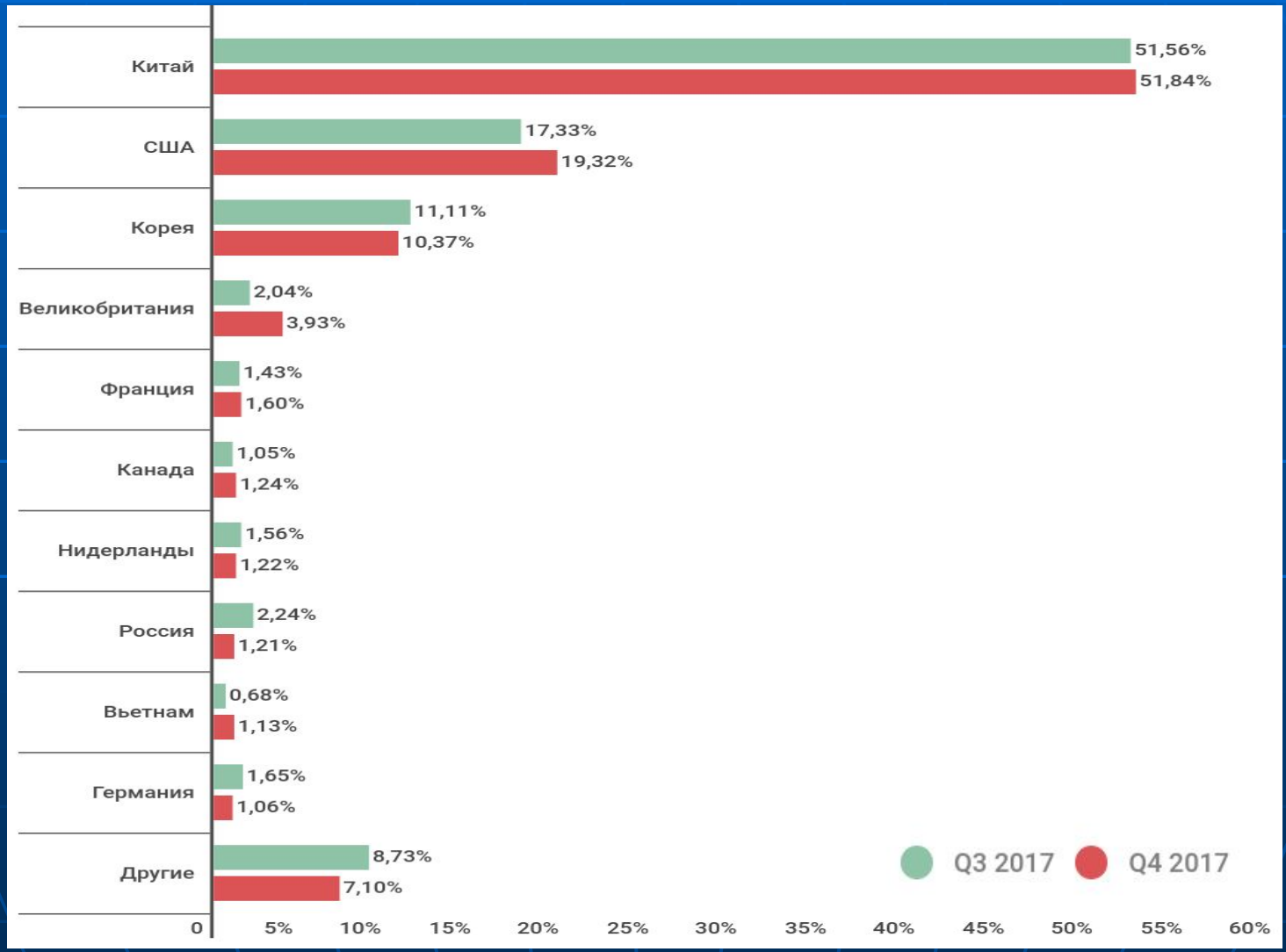
- Distributed Denial of Service — распределенная атака типа «отказ в обслуживании»
- проводится с нескольких компьютеров.
- используется ботнет, состоящий из зараженных компьютеров или устройств IoT.

IoT

- **Internet of Things**
  концепция вычислительной сети физических предметов (*«вещей»*), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой.

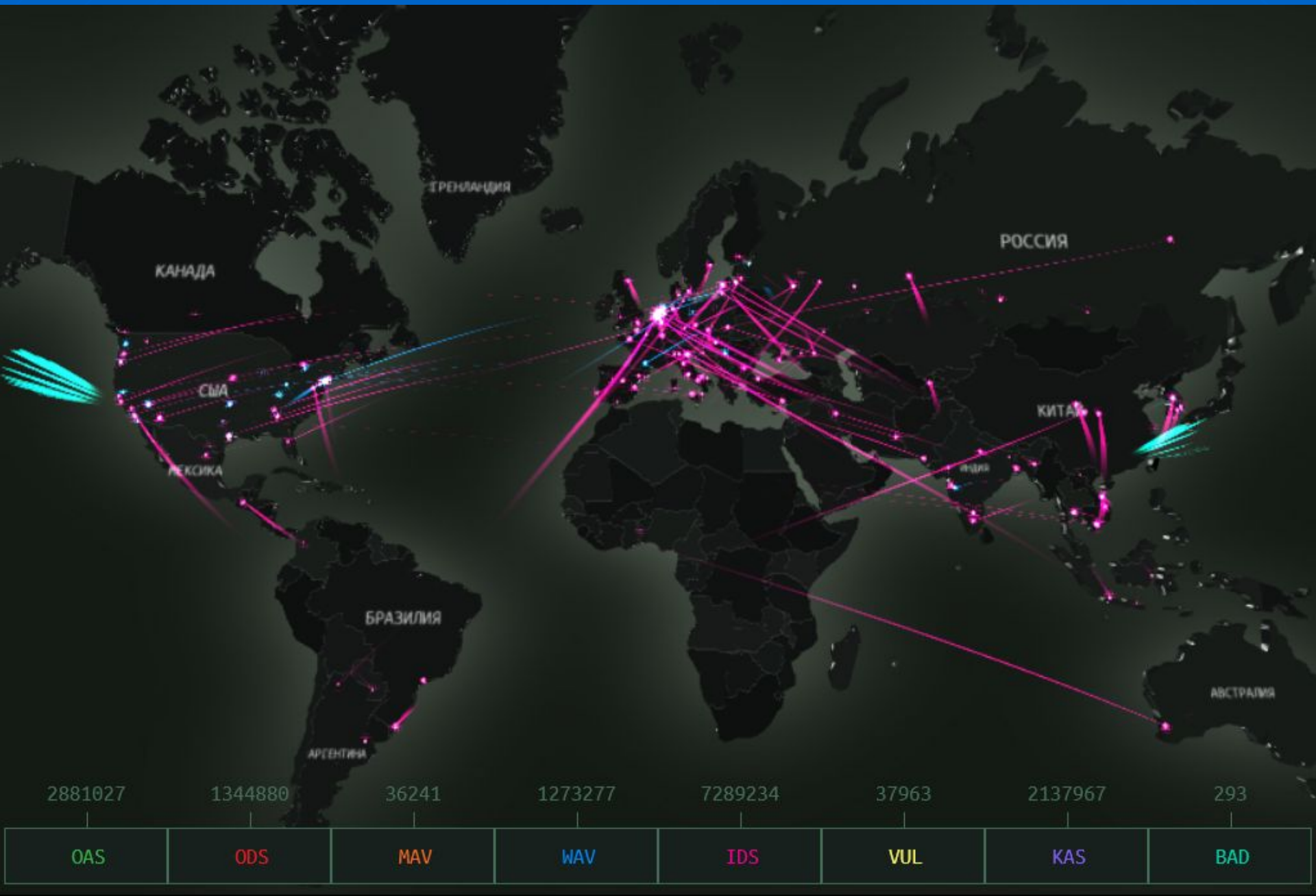
- **Internet of Things** концепция вычислительной сети физических предметов (*«вещей»*), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой.

КОГО АТАКУЮТ



КОГО АТАКУЮТ

- В первом полугодии 2017 года число атак на IoT-устройства возросло на 280%
- 25–26.02.2018 - атака полосой 480 Гбит/с платежная система QIWI


ГРЕНЛАНДИЯ
КАНАДА
РОССИЯ
США
КИТАЙ
МЕКСИКА
БРАЗИЛИЯ
АВСТРАЛИЯ
АРГЕНТИНА
2881027
1344880
36241
1273277
7289234
37963
2137967
293
OAS
ODS
MAV
WAV
IDS
VUL
KAS
BAD

Вирусная активность

AVG		
1	Adware Generic	16.99%
2	Adware Generic_r	4.70%
3	Fake Update	4.48%
4	MyBackup	3.03%
5	BundleApp_r	1.76%

Dr.Web		
1	SCRIPT.Virus	2.11%
2	Trojan.Packed.24524	0.81%
3	Trojan.Triosir.13	0.57%
4	BackDoor.Andromeda.404	0.51%
5	Tool.NetFilter.1	0.49%

Kaspersky		
1	DangerousObject.Multi.Generic	15.08%
2	Trojan.Win32.AutoRun.gen	7.40%
3	Worm.VBS.Dinihou.r	6.58%
4	Trojan.Win32.Generic	6.50%
5	Net-Worm.Win32.Kido.ih	5.09%

СПАМ

анонимная, массовая почтовая корреспонденция нежелательного характера

76,2%

от всего почтового трафика

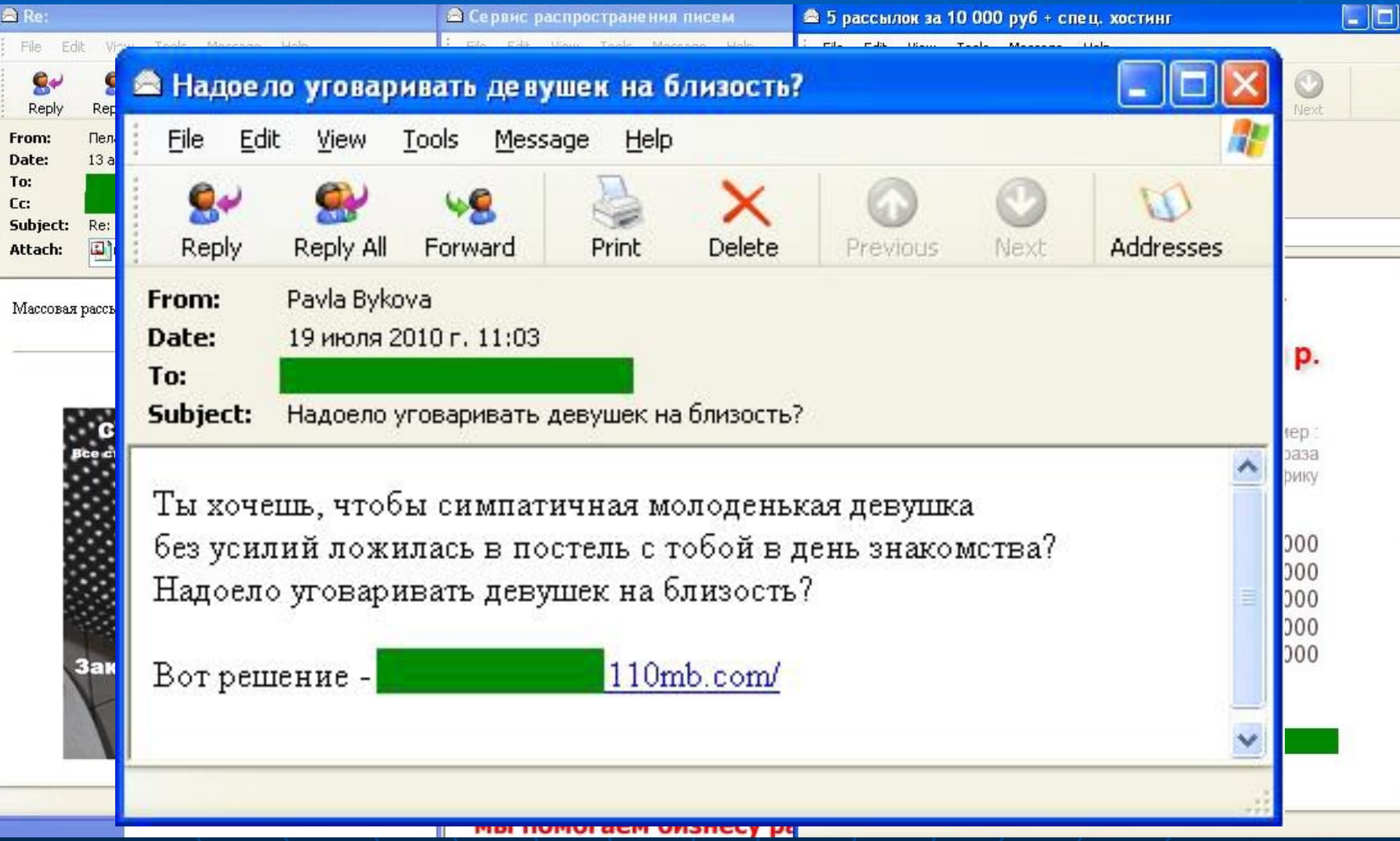
СПАМ


"Лаборатория Касперского"
12,4%
11,0%
9,7%
6,5%
5,9%
3,7%
3,6%
3,2%
2,9%
2,6%
2,0%
1,8%
1,8%
1,5%
1,7%
1,3%
1,4%
1,2%
1,2%
1,3%
24,4%
Индия
Индонезия
Бразилия
Перу
Корея (Южная)
Вьетнам
Италия
Польша
Колумбия
Аргентина
Украина
Казахстан
Тайвань
Россия
Испания
США
Великобритания
Франция
Саудовская Аравия
Румыния
Другие

СПАМ

Спам-тематика декабря 2011:

СПАМ


Re:
Сервис распространения писем
5 рассылок за 10 000 руб + спец. хостинг
Надоело уговаривать девушек на близость?
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: Pavla Bykova
Date: 19 июля 2010 г. 11:03
To: [redacted]
Subject: Надоело уговаривать девушек на близость?
Ты хочешь, чтобы симпатичная молоденькая девушка
без усилий ложилась в постель с тобой в день знакомства?
Надоело уговаривать девушек на близость?
Вот решение - [redacted] 110mb.com/

«Нигерийские» письма

«Нигерийский» спам — это разновидность компьютерного мошенничества, попытка под неким вымышленным предлогом получить доступ к банковскому счету пользователя или иным путем получить с него деньги.

YUKO\'S OIL. - Western European (ISO)

File Edit View Tools Message Help

From: vkchambers
Date: 18 октября 2004 г. 14:10
To:
Subject: YUKO\'S OIL.

Good day ,

I Barrister Miroslav Vlado Khodo, representing Mr.Mikhail Khodorkovsky
(m.k.) of Russia. He is one time the richest man in Russia and the head of
YUKO'S OIL till that unfaithful day that they got him arrested and since
then all his accounts and known businesses have been confiscate. I would
like to ask for your partnership in re-profiling funds over US$42 million.
I will give the details, but in summary, the funds are coming via bank transfer.
Please note that as an attorney I want a very straight forward and God fearing
person as this is a legitimate transaction and not a Child play. You will
be paid 10% for your "management fees". You can log into
this web site to

PLEASE I NEED YOUR HELP - Western European (ISO

File Edit View Tools Message Help

From: sussan1 dunga
Date: 26 августа 2005 г. 12:42
To:
Subject: PLEASE I NEED YOUR HELP

PLEASE I NEED YOUR HELP
MISS SUSSAN DUNGA,
ABIDJAN,COTE D'IVOIRE,
FROM SUSSAN DUNGA,

My name is Miss Sussan dunga. The only daughter of Late General Mohammed dunga the former Director of military inteligence and special acting General Manager of the Sieria Leone Diamond mining coperation (SLDMC). I am contacting you to seek your good assistance to transfer and invest USD 18 million belonging to my late father which is deposited in a bank in Abidjan. This money is revenues from solid minirals and diamonds sales which were under my fathers possession before the civil war broke out.
Following the brake out of the war, almost all government offices, coperations and parastatals were attacked and vandalized. The (SLDMC) was loothed and burnt down to ashes, and diamonds worth millions of dollars was stolen by the rebel military forces who attacked my fathers office.Many top government officials and
senior army officers were assasinated and my father was a key target because of his very sensitive military possition and appointment in the (SLDMC).Regreatably,my father was captured and murdered along with half brother in cool blood during a mid-night rebel shoot-out when our official residence in freetown was armbushed by Fordey Sanko the

Помогите нигерийскому космонавту

Dr. Bakare Tunde Astronautics Project Manager National Space Research and Development Agency (NASRDA) Plot 555 Misau Street PMB 437 Garki, Abuja, FCT NIGERIA

Dear Mr. Sir, REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989.

He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost $ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost $ 3,000,000 American Dollars. In order to access his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course. Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter. Please acknowledge the receipt of this message via my direct number 234 (0) 9-234-2220 only. Yours Sincerely, Dr. Bakare Tunde Astronautics Project Manager

Поздравляем, вы выиграли! или Что скрывается за лотереями в интернете

From: DR.GRAIG WILLIAMS <cocacolaclaimsdepartmentukfr1@yahoo.fr>
Subject: Winmner

ONLINE COCA COLA COMPANY.
PO Box 1010,
Liverpool L70
1NL, United Kingdom,

Dear Winner,
this is Winner's Invitations from Coca Cola Company Promo. Kindly Contact Your Claims Agent DR. GRAIG WILLIAMS for direction on how to claim your prize in this week. From now onward you will be receiving our promotional offers and survey invitations from Coca Cola Company..... (You can unsubscribe at any time.) We want you to remove skepticism from your mind because this award is legitimate from COCA COLA COMPANY PLC, ENGLAND. Most importantly this is to let you know that you are a winner of the sum of 500,000.00GBP (Five Hundred Thousand Great British Pounds Sterling's) in this runner up. Please make sure your prize is claimed urgently.
Congratulations!
ONLINE COCA COLA COMPANY.

Поздравляем, вы выиграли! или Что скрывается за лотереями в интернете

Как понять, что перед вами письмо от мошенника?

Ответ:

любое уведомление о выигрыше в лотерею,
в которой вы **не участвовали**, — **поддельное**.

Поздравляем, вы выиграли! или Что скрывается за лотереями в интернете

Простые правила безопасности:

1. Не верьте, что вы могли выиграть денежный приз, в розыгрыше, в котором вы не участвовали.
2. Не доверяйте письмам, "прогнанным" через автоматический переводчик или просто содержащим явные ошибки.
3. Обращайте внимание на e-mail, с которого прислано сообщение: организаторы лотерей не отправляют письма с бесплатных почтовых сервисов.
4. Если вы думаете, что все-таки в письме речь идет о реальном выигрыше, проверьте все данные с помощью поисковых систем. Имена и телефоны отправителей, название лотереи — все это, возможно, найдется в Сети с подробными комментариями.
5. И самое главное, помните: бесплатный сыр бывает только в мышеловке!

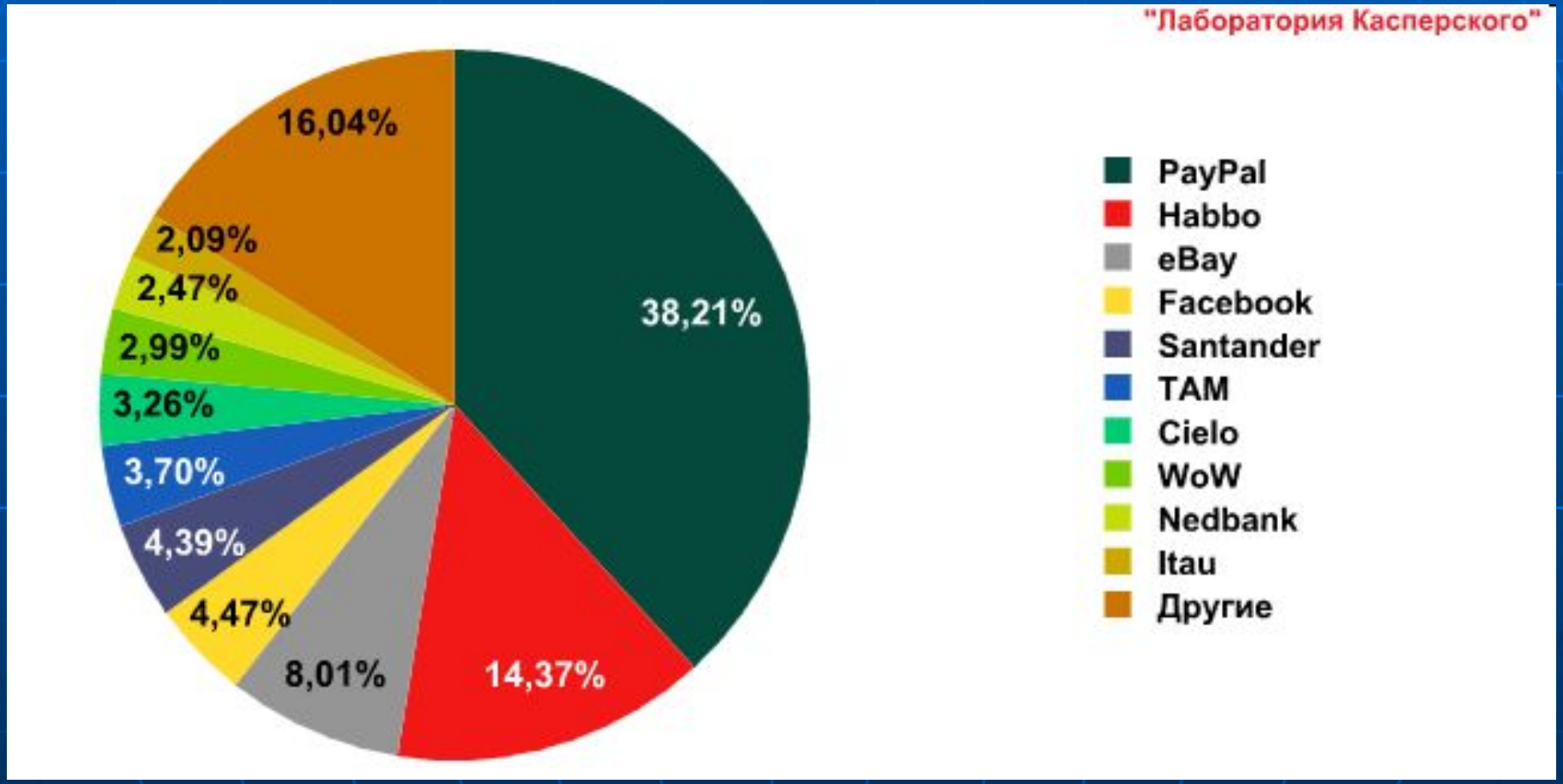
Фишинг (Fishing)

- Создание сайта с похожим названием с целью кражи пароля и логина пользователя.
- Пример:

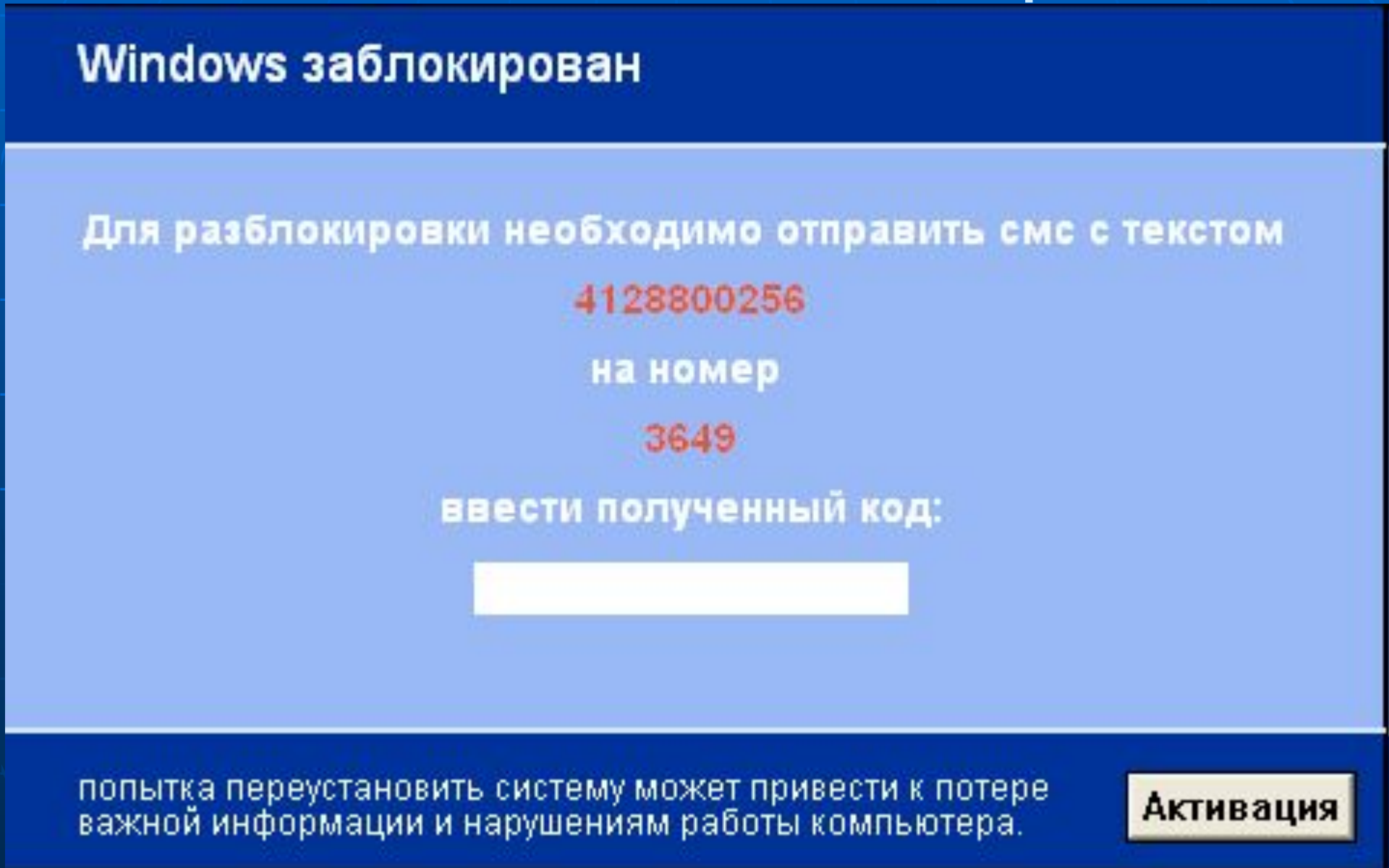
www.mail.ru

www.mai1.ru

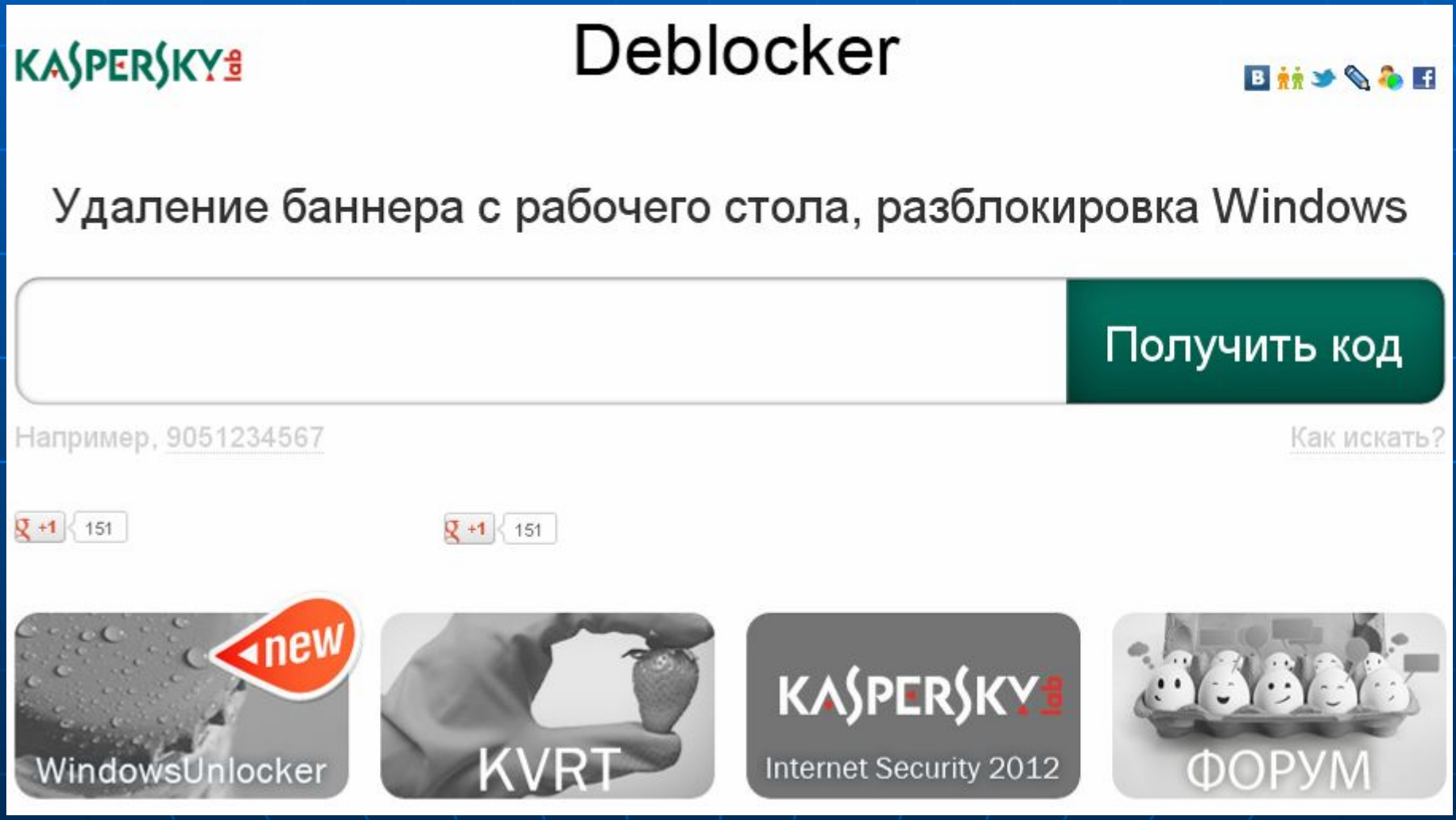
Фишинг (Fishing)



Вымогатели-блокеры



Сервис деактивации вымогателей-блокеров http://sms.kaspersky.ru



www.drweb.com/xperf/unlocker/?lng=ru

Помощь

Звоните бесплатно в России:
8–800–333–7932

Задать вопрос

Прислать вирус

Частые вопросы

Форумы

Дешифровка от Trojan.Encoder

Разблокировка Windows (Trojan.Winlock)

Аптечка сисадмина

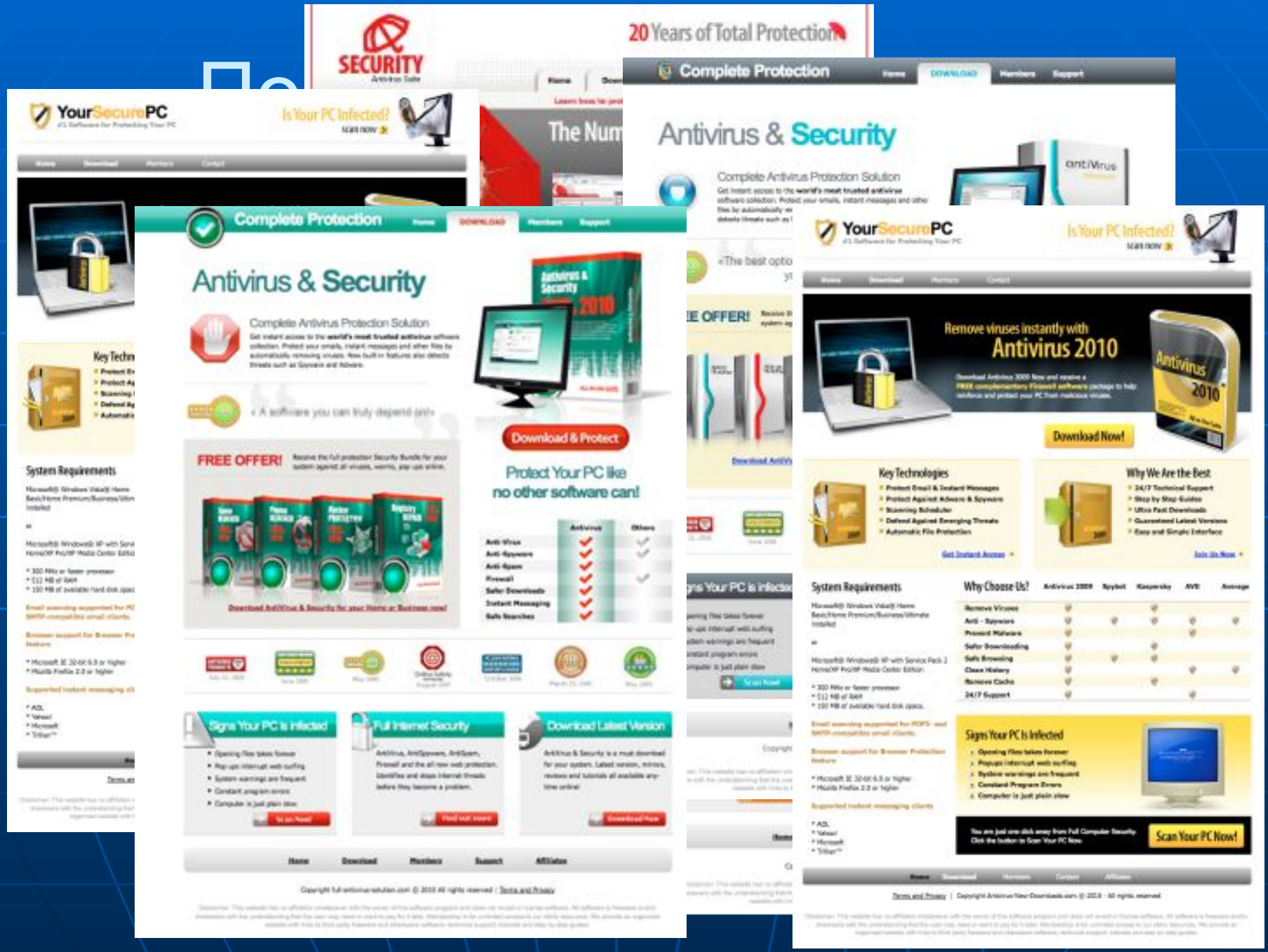
Для бета-тестеров

Сервис разблокировки компьютеров

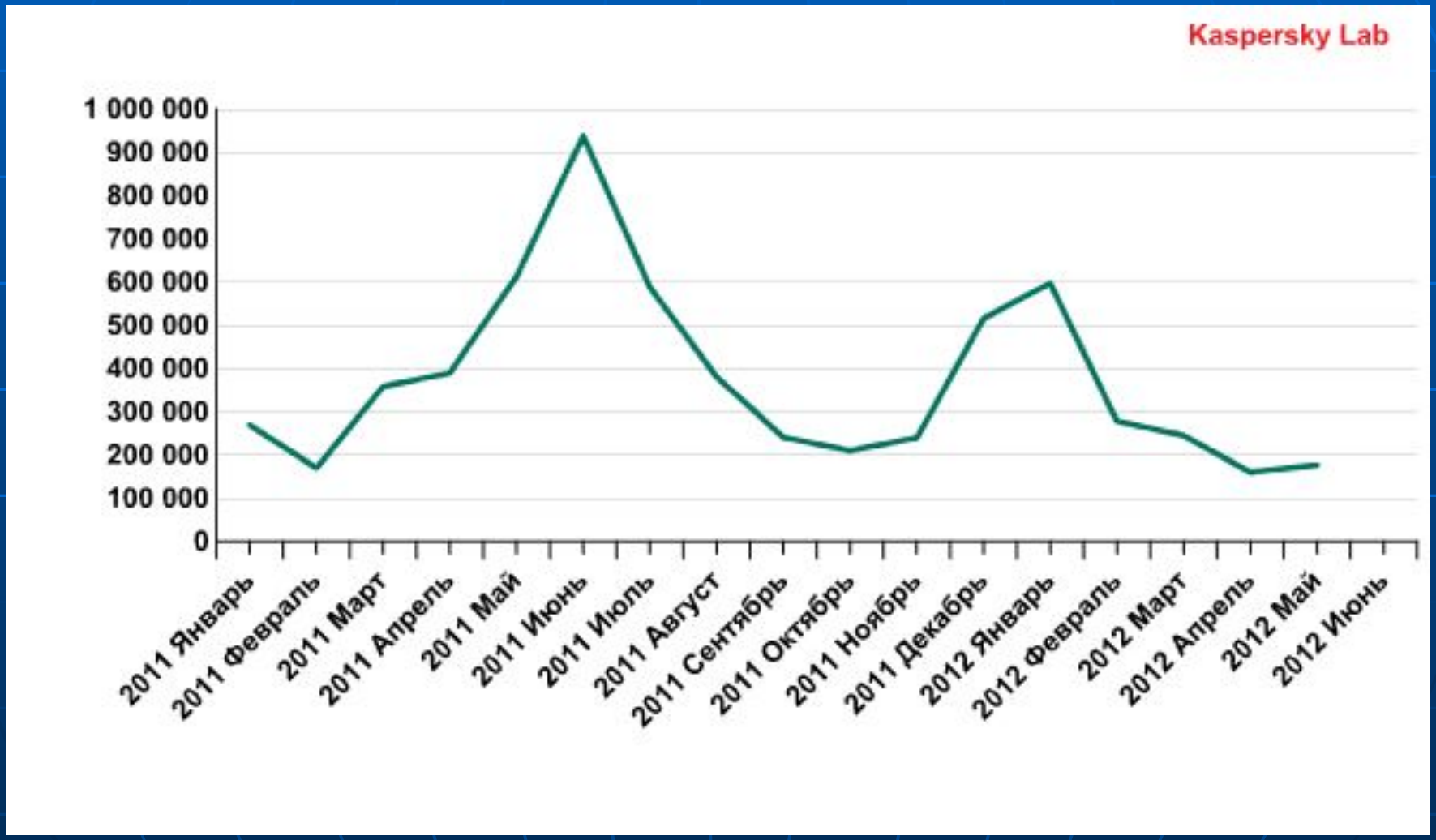
Введите номер кошелька/телефона

Искать коды

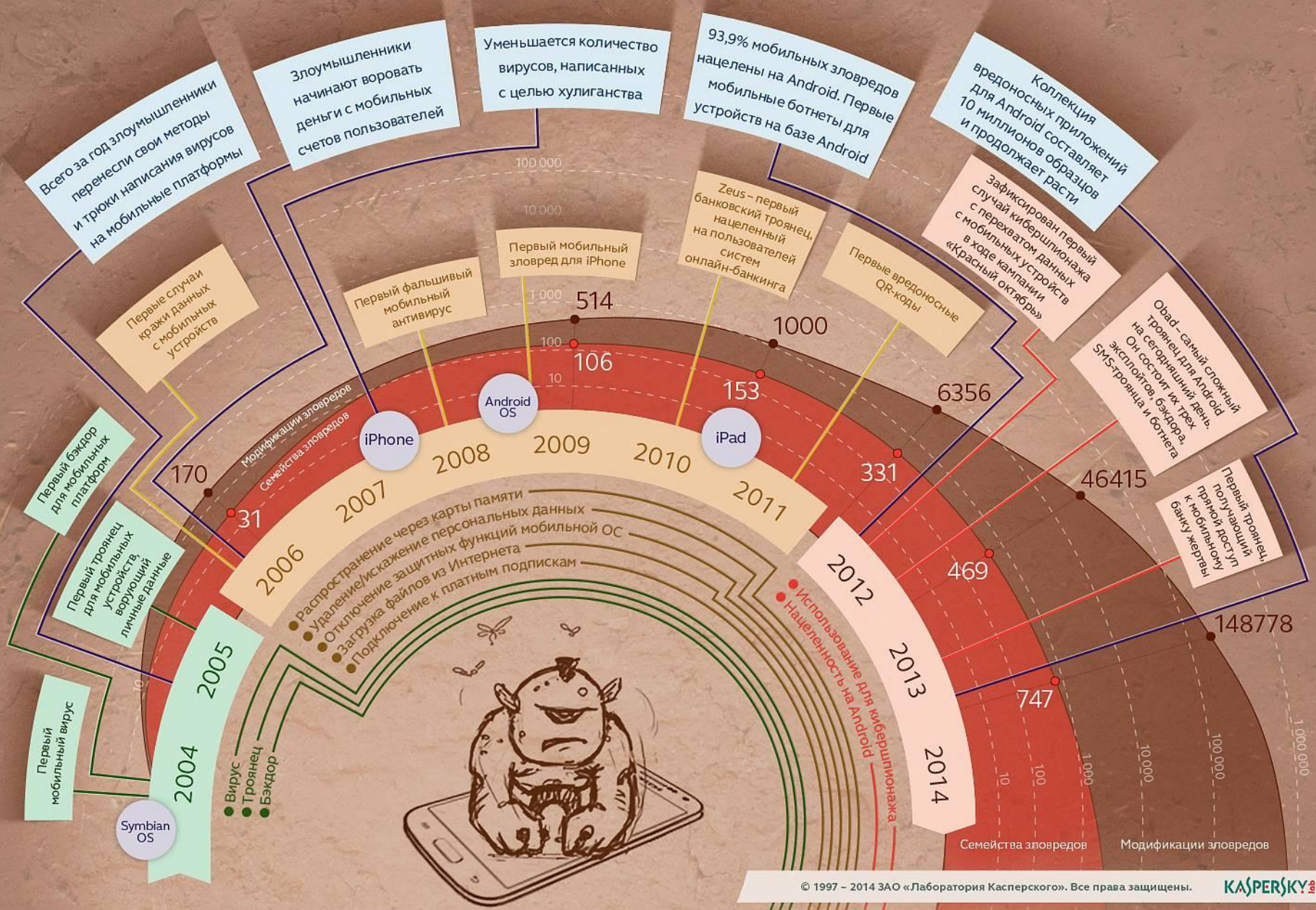
Попробуйте подобрать код и название вируса по изоб


SECURITY
20 Years of Total Protection
YourSecurePC
Is Your PC Infected?
Complete Protection
Antivirus & Security
Complete Antivirus Protection Solution
Download & Protect
Protect Your PC like
no other software can!
FREE OFFER!
Remove viruses instantly with
Antivirus 2010
Download Now!
Key Technologies
Why We Are the Best
System Requirements
Why Choose Us?
Signs Your PC is Infected
Scan Your PC Now!

Подозрительный файл



Эволюция мобильных зловредов



KASPERSKY lab

Антивирусная защита

- Антивирус Касперского - www.kaspersky.ru
- Dr.Web – www.drweb.ru
- Nod32 – www.esetnod32.ru
- Avast - www.avast.com
- и др.

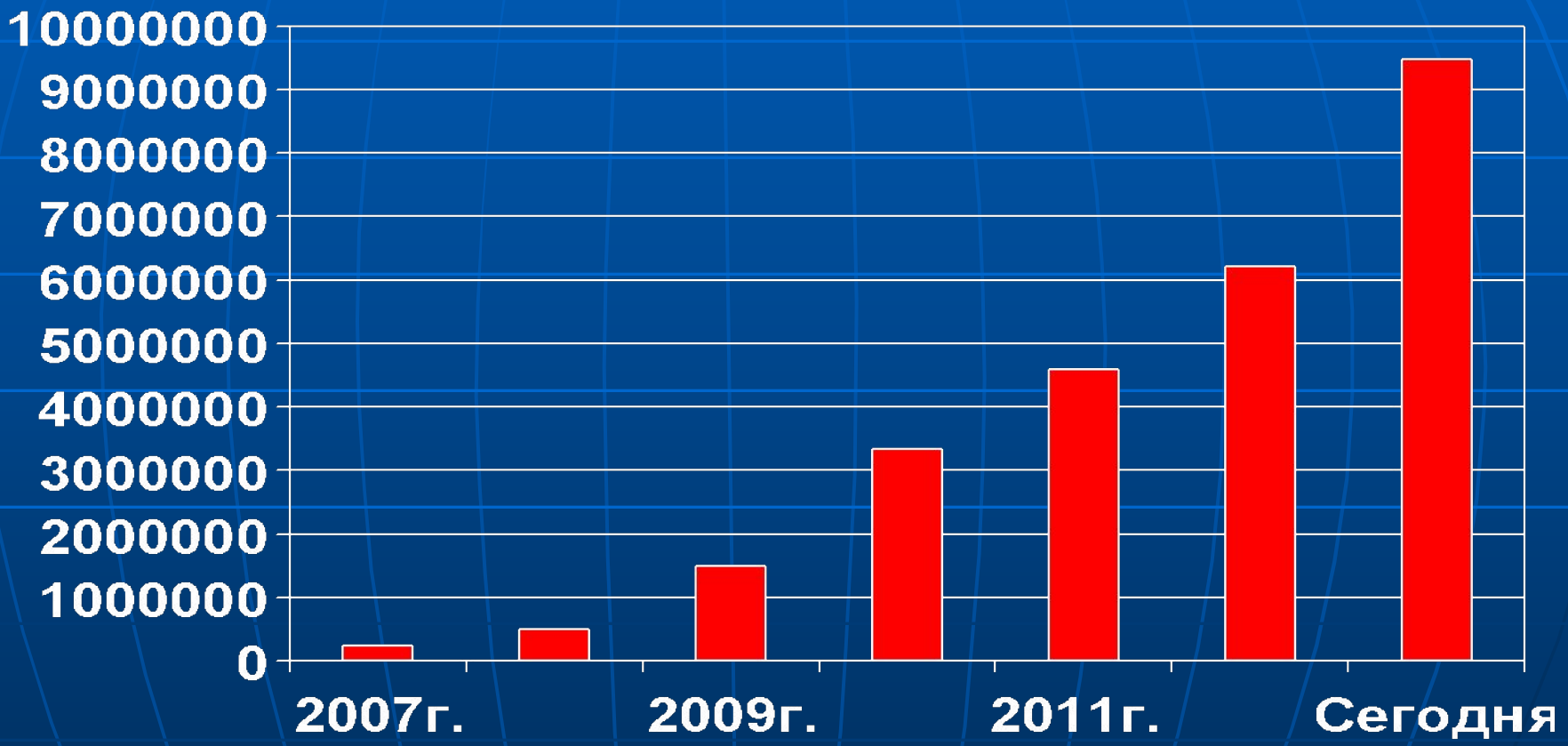
Обнаружение и блокирование

1. реактивный – метод, основанный на поиске вредоносных объектов с помощью постоянно обновляемых баз приложения.

Обнаружение и блокирование

2. проактивный – нацелен на обнаружение новых угроз, информации о которых еще нет в базах. Основан на анализе поведения вредоносных объектов в системе.

Количество вредоносных объектов



Количество вредоносных объектов

28822 - вредоносные скрипты
1086439 - фишинговые сайты
29771 - баннеры
95511 - спам
1212 - сетевые атаки
9 480 318 - вредоносные программы

19. 02. 2013

Количество вредоносных записей

5439

В среднем за 1 сутки

Количество вредоносных объектов

лето 2009

FreeBSD - 43

OSX - 48

Sun Solaris - 119

Unix - 212

Linux - 1898

Windows - 2247659

Защита

1. Установить **антивирус**
2. Установить Программу Panda USB Vaccine
   - На флешке создает файл **autorun.inf**
   - Отключает **автозапуск** на компьютере
3. Проверить файл **hosts**
4. Скачать бесплатную утилиту

   Dr.Web CureIT! ИЛИ

   Kaspersky Virus Removal Tool

Ресурсы по безопасности

www.saferunet.ru – национальный узел интернет – безопасности в России.

www.securelist.ru – описание вирусов.

www.securitylab.ru – новости по информационной безопасности.

БЕСПЛАТНАЯ УТИЛИТА

http://devbuilds.kaspersky-labs.com/devbuilds/AVPTool/
www.freedrweb.com/download+cureit/gr/

ПРОВЕРКА ПОДОЗРИТЕЛЬНЫХ ФАЙЛОВ

http://support.kaspersky.ru/viruses/online

https://vms.drweb.com/sendvirus/

www.virustotal.com – разными антивирусами

LiveCdUsb

- Dr.Web LiveCD
- Kaspersky Rescue Disk
- Avira Rescue CD
- eScan Rescue Disk
- Comodo Rescue Disk
- AVG Rescue CD

http://freeprotection.ru/livecdusb/