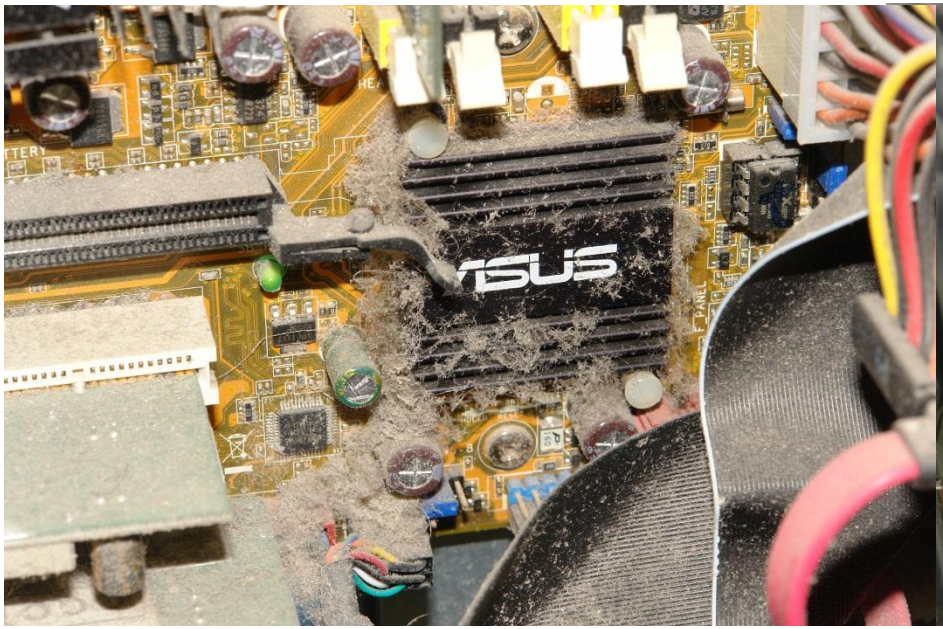
Методы и средства защиты компьютерной информации
Информационная безопасность и защита информации

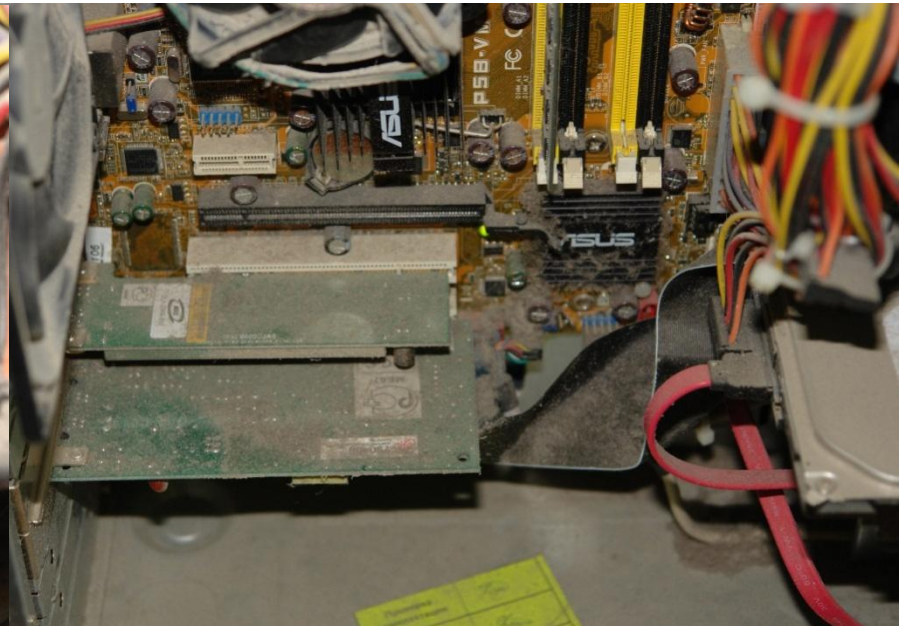
Лектор: Преображенский Юрий Петрович

Доцент, кандидат технических наук

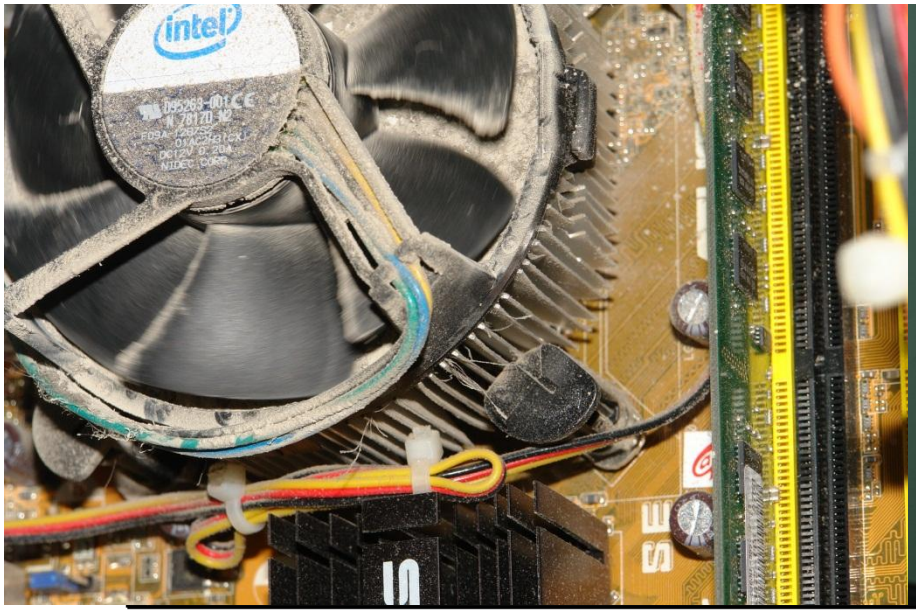
Раздел первый

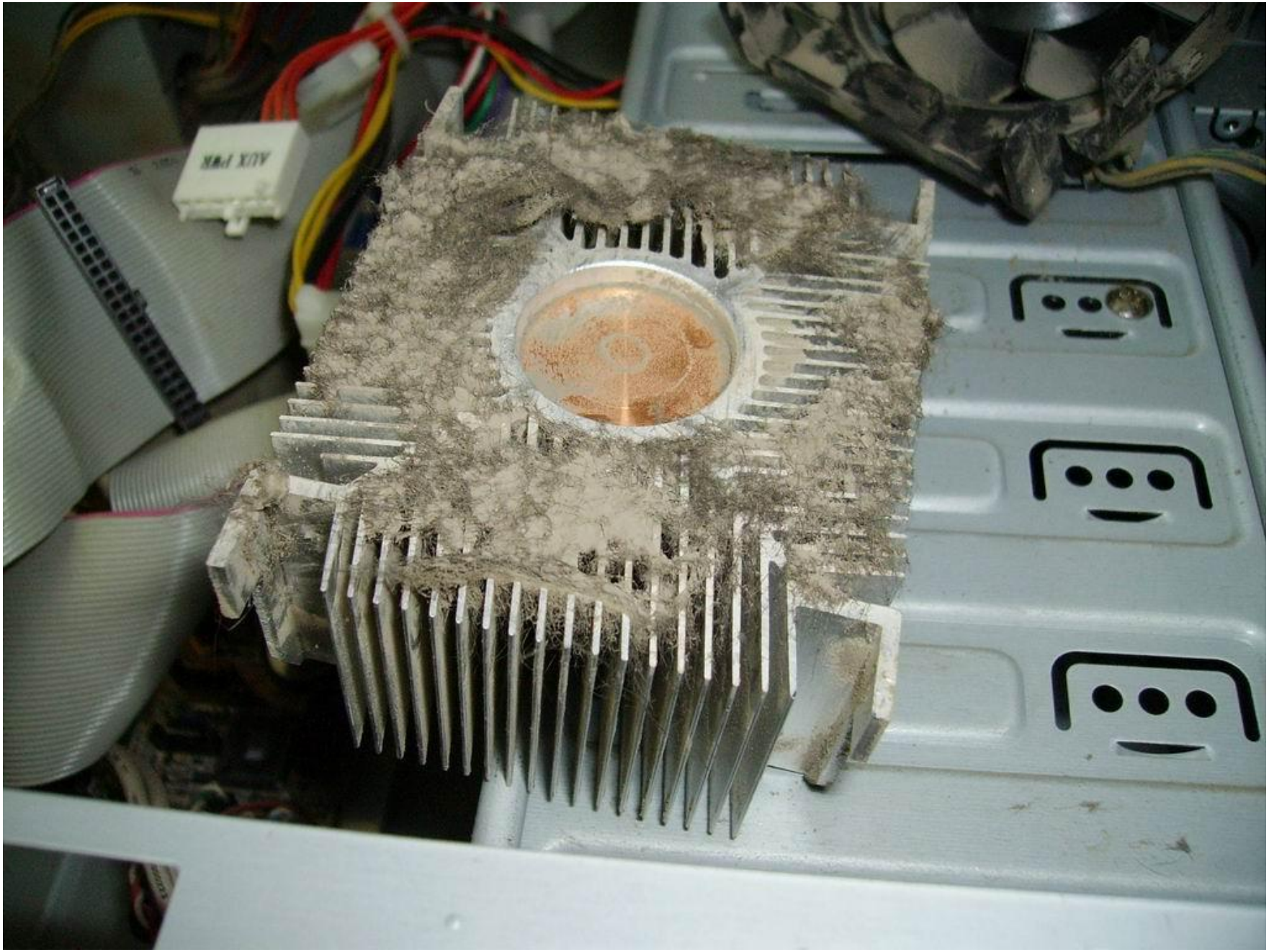
«Введение в основные положения теории информационной безопасности»

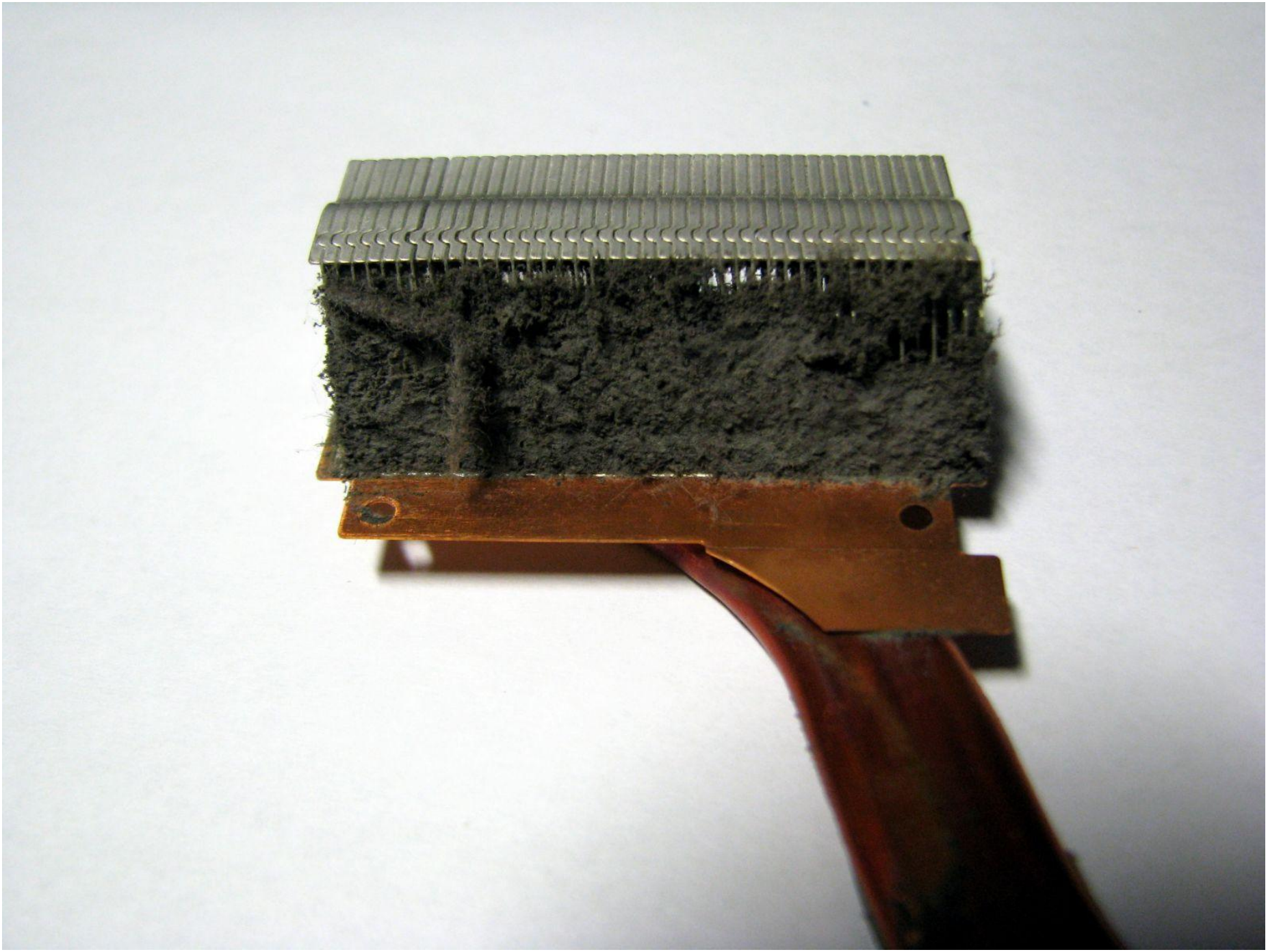




Системник, который никто и никогда не чистил…




AUX PWR



Современная ситуация в области информационной безопасности

Статистика инцидентов, связанных с информационной безопасностью

За 2013 год специалистами в области компьютерной безопасности

- обнаружено и обезврежено свыше 4000000000 вредоносных объектов.

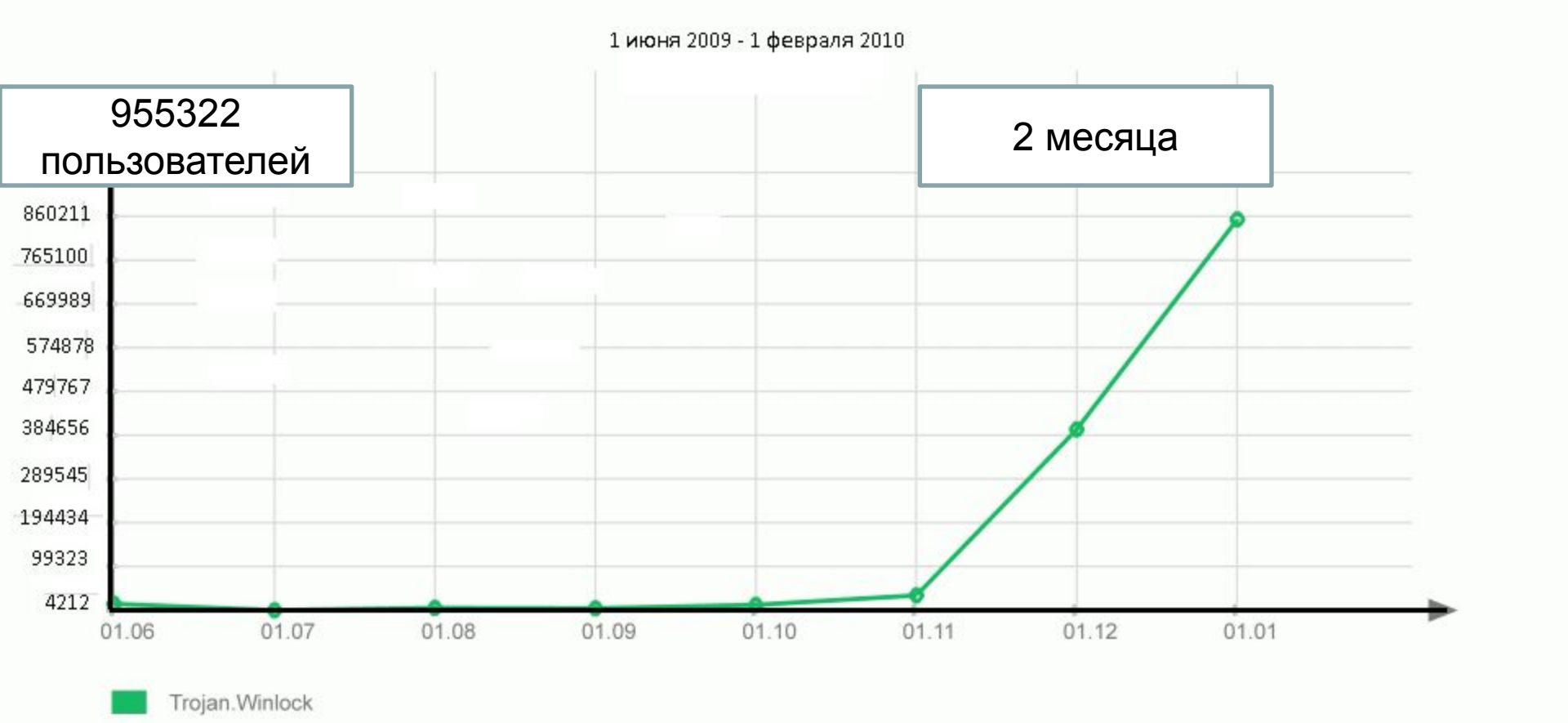
- обнаружено более 80000 новых модификаций вредоносных программ для мобильных устройств

Adobe

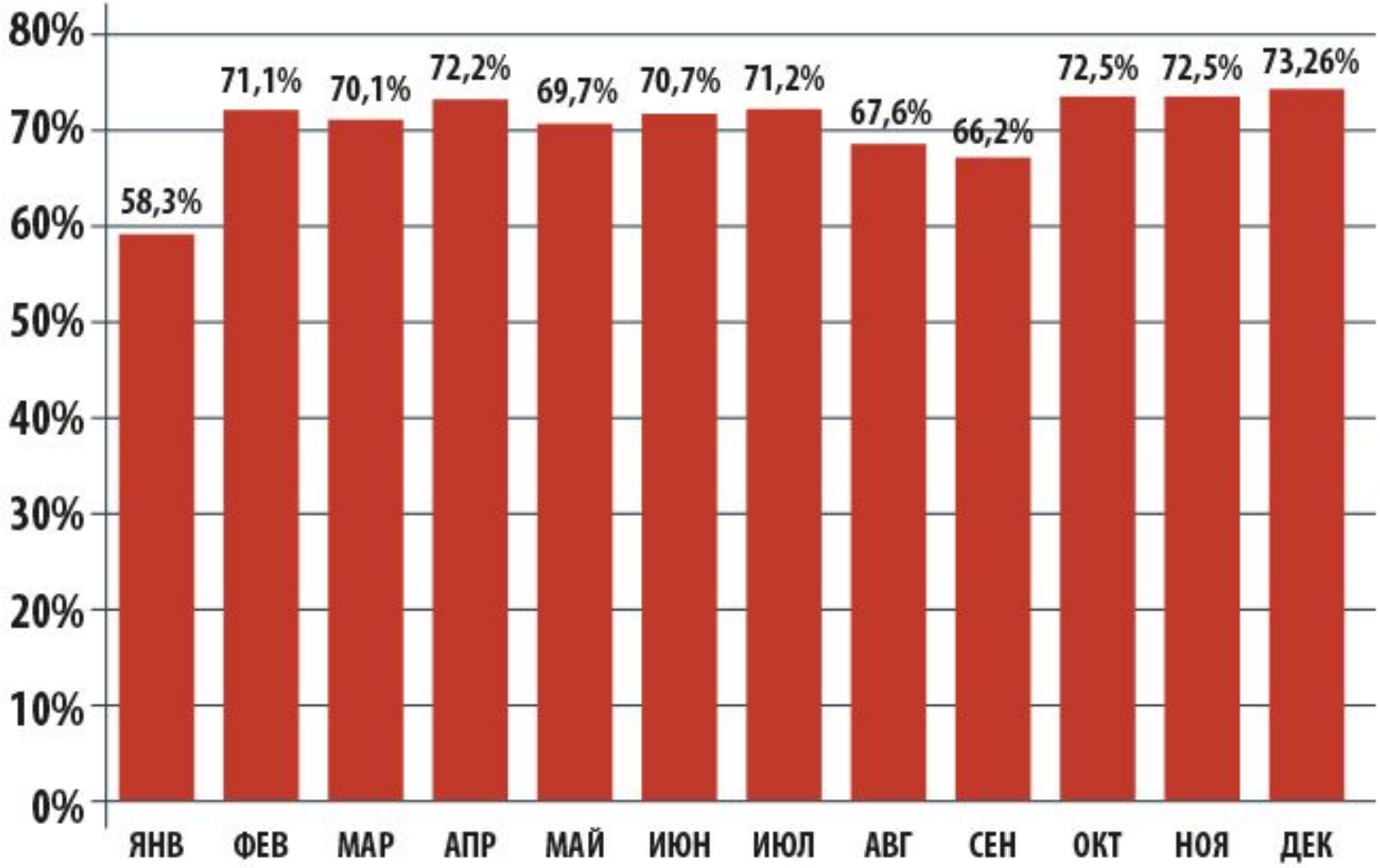
- около 40% отраженных эксплойтов используют уязвимости в продуктах компании Adobe.

- около 70% всех вредоносных хостов расположено в четырех странах: в США, России, Китае и в Нидерландах.

Статистика заражения вирусом Trojan.Winlock за 8 месяцев



Доля спама в российском сегменте Интернет, 2013



@131.178.c10008-a77.dsl-dynamic.vsi.ru
@189-69-121-39.dsl.telesp.net.br
@209-11-95-178.pool.ukrtel.net
@3brenda.ru
@a2zlearning.org
@aaghoshpakistan.org
@aapfco.org
@ableekertomorrow.com
@abramovsky.ru
@ac18.org
@academiadecienciasrd.org
@acfcca.org
@acimc.org
@ackbar.org
@acme.org
@acmhddsa.org
@activatedusa.org
@actlibya.org
@adi-macedonia.org
@adio.org
@adoc.net
@ae.org
@afr-sd.org
@agcne.org
@aice.org
@aites.net
@ala-choice.org
@alaluzdelabiblia.org
@alanonsofla.org
@alaskafisherman.com
@albadr-alkamel.org
@aleek.org
@alexworld.org
@alianza-almeria.org
@alilmemrc.org
@allenorchestra.org
@allentowncorvetteclub.org
@allianceimaging.org
@alltasks.com
@almaswanwatch.org
@alpha-kappa-delta.org
@alphasigmaalpha.org
@altra.org
@alumniblueband.org
@amstat-online.org
@anadhavidyarthigriha.org
@andersonmori.com
@anewamerica.org
@ashland.org
@asnro.ioffe.ru
@ats.lv
@audiostatic.com
@autobereg.ru
@autobustur.ru
@avalon-tek.ru
@avtomiass.ru
@avtounion.ru
@baltic-gold.com
@barrylevin.com
@bezdyma.ru
@blacktusk.org
@blanchardscutlery.com
@blazic.com
@blmail.ru
@bloss.org
@bondex.ru
@bonita.net
@booksir.com
@bridson.com
@btsg.net
@canders.com
@canes.ru
@capamail.ru
@capitalreg.ru
@cgee.com
@chapelvalley.com
@chemstress.com
@cheremushki.od.ua
@chins.ru
@chorn.net
@christopher.net
@cmoi.com
@co.uk
@confetticonverters.com
@contessa.co.uk
@contrato.ru
@crippa.org
@dalnews.com
@databusters.net
@dccmail.ru
@dechc.org
@dewalt.ru
@dexter.org
@digex.com
@divan.com.ru
@doctorm.com
@drakesystemsgroup.com
@dthompson.de
@duitz.com
@dvm-tour.ru
@eelectro.ru
@ekos1.ru
@eltanin.net
@ep.uz
@erahomeandfamily.com
@ethreemail.com
@euro44.ru
@euro-football.ru
@express.dn.ua
@fargotm.ru
@fewmets.net
@fiberglassusa.com
@fidtech.ru
@financereg.ru
@fininterpost.ru
@finitlaw.com
@finkursy.ru
@fiorino.org
@flatline.de
@focalpaper.com
@forward-mebel.ru
@fraser.org
@frezza.de
@fun-y.ru
@gernaboyz.com
@ghtlawyers.com
@goldner.com
@govind.de
@gravotek.ru
@gronk.com
@group.omotokai.jp
@header.com
@healthy.co.uk
@help-student.ru
@herky.net
@h-o-d.ru
@holdmail.ru
@host-46-186-73-191.dynamic.mm.pl
@hosting-reseller.ru
@hotel-olymp.ru
@hr-solutions.com
@h-wave.com
@idsoftcapital.com
@ieee.de
@iloveglam.com
@imalc.com
@intrago.com
@iparfum.ru
@ireland-rentals.com
@jacksongroup.com
@janpr.jnj.com
@jdata.ru
@jericho.org
@jobedupost.ru
@johnrossjr.com
@kadochnikov.ru
@kdn.ktguide.com
@kordio.ru
@kroy.org
@kursmail.ru
@lammlilocke.com
@lanai.intrnic.com
@landmarkdevelopmentco.com
@listedumail.ru
@mail2k.ru
@mail2matthew.com
@millenniumag.com
@millshassall.com.au
@moivrach.ru
@mtkpost.ru
@my.nestle.com
@myerp.ru
@myunseenworld.com
@nanb.com
@nebo9.ru
@netgen.com
@nextmail.ru
@niagaraspas.ru
@nicomatic.com
@nm.ru
@nxt.ru
@nynex.de
@office.ikirov.ru
@offshorecyprus.ru
@pan-cargo.com
@personalhelp.co.uk
@perulaptop.com
@pimapenkomi.ru
@portedumail.ru
@powerschapman.com
@poxod.ru
@pravo-info.ru
@prim.fsgs.ru
@qrtol.com
@rael-letson.com
@ranchoweb.com
@relivinc.com
@reslist.ru
@reud.ru
@rivercitygroup.com
@rivernet.net
@rjy.com
@rlgsc.com
@rosslevinedesign.com
@rusotdih.ru
@sandy.ru
@schwerhoerigkeit.de
@semlist.ru
@semopt.ru
@shokoladki.ru
@sinko.kiev.ua
@sinteg.ru
@skif.zp.ua
@sls-consult.com
@softforall.ru
@sovietrally.ru
@spbcomail.ru
@spbedumail.ru
@sputnikmag.ru
@statesmanbiz.com
@swfcompanies.com
@systemail.ru
@tetramarket.ru
@text.telus.com
@timelogic.ru
@tlcd.com
@tourbaikalland.ru
@treske.com
@triband-mum-120.60.25.54.mtnl.net.in
@uermz.ru
@ulmart.ru
@uswi.com
@vacmail.ru
@vanna.ru
@vedboard.ru
@vendome.com
@vestnikineta.ru
@vokspb.ru
@wazup.com
@wengier.com
@winston.ru
@wlxn.com
@wmod.ru
@wsewopost.ru
0usj1s8@inbox.ru
2hronai@mail.ru
4ybmco5@qip.ru
6iay2@mail.ru
74bbo@bk.ru
7cai5@rambler.ru
7utxtn@list.ru
8ceusv@bk.ru
9qkaxw3@list.ru
9vrod@list.ru
9wbasx@mail.ru
achh@qip.ru
ai3tdw5@inbox.ru
alexis.lamborgini@mail.ru
allowancesg59@qip.ru
alta.aaccf@mail.ru
alyssa.lamborgini@mail.ru
amandi.aaccf@mail.ru
anaytzvsim@mail.ru
angel.infinity@mail.ru
annabel.aaccf@mail.ru
appendedp683@inbox.ru
apurve.aaccf@mail.ru
architecturalniwa4@bk.ru
ardys.aaccf@mail.ru
asvl@rambler.ru
atsuo.aaccf@mail.ru
avuyzmp@yandex.ru
b1kk0@bk.ru
badri.octavia@mail.ru
banachxak34@ya.ru
baominh.aaccf@mail.ru
berger.octavia@mail.ru
bestactspenmo@fromru.com
bjq5y@qip.ru
brownstonebw3@list.ru
btlosot@mail.ru
c6buo@bk.ru
cammi.aaccf@mail.ru
carlota.aaccf@mail.ru
carmelina.octavia@mail.ru
carmen.aaccf@mail.ru
carolyne.aaccf@mail.ru
carter.aaccf@mail.ru
caterina.aaccf@mail.ru
cathyleen.aaccf@mail.ru
cboddw@yandex.ru
celle.aaccf@mail.ru
cesar.aaccf@mail.ru
cheslie.aaccf@mail.ru
confrontationss4@ya.ru
crystal.aaccf@mail.ru
dakghwv@rambler.ru
damara.aaccf@mail.ru
darda.aaccf@mail.ru
dctcnyn@bk.ru
debyh65@list.ru
demetris.aaccf@mail.ru
distz6@inbox.ru
donnie.aaccf@mail.ru
duljit.infinity@mail.ru
earl.infinity@mail.ru
ebonics30@inbox.ru
eeyb@mail.ru
efdal.aaccf@mail.ru
eleonore.aaccf@mail.ru
elsie.infinity@mail.ru
elyn.aaccf@mail.ru
emerson.aaccf@mail.ru
emylee.aaccf@mail.ru
eq77lkp@bk.ru
erik.aaccf@mail.ru
evie.aaccf@mail.ru
fdxn8v@list.ru
felecia.aaccf@mail.ru
felipe.aaccf@mail.ru
ffx1g@yandex.ru
fghy@inbox.ru
fi8dn@list.ru
freida.octavia@mail.ru
fx57mcb@mail.ru
gammasvrl837@gmail.com
gerhard.aaccf@mail.ru
gerikhanpqqso@mail.ru
geza.infinity@mail.ru
gghxk7@inbox.ru
gkogxnw@qip.ru
glornia.octavia@mail.ru
glossedsu04@narod.ru
gracie.aaccf@mail.ru
gsgi@yandex.ru
guenevere.octavia@mail.ru
gylw@yandex.ru
hazem.octavia@mail.ru
heidie.aaccf@mail.ru
hiqgjlm@yandex.ru
hoa.aaccf@mail.ru
hodgdcoundevra@fromru.com
holly-anne.aaccf@mail.ru
hopeduk0@gmail.com
hulda.aaccf@mail.ru
ibby.infinity@mail.ru
impeji@list.ru
impose022@gmail.com
incrediulouslyub90@ya.ru
infatuatednlh2@yandex.ru
jawad.aaccf@mail.ru
jean-normand.aaccf@mail.ru
jnkc@yandex.ru
jo-anne.aaccf@mail.ru
jocelin.aaccf@mail.ru
jody.aaccf@mail.ru
kad7yr@bk.ru
kally.aaccf@mail.ru
karolina.infinity@mail.ru
kevina.infinity@mail.ru
lanette.aaccf@mail.ru
larderspn865@yandex.ru
laurie.aaccf@mail.ru
leonas.infinity@mail.ru
lexine.octavia@mail.ru
lianne.infinity@mail.ru
lola.aaccf@mail.ru
lon.infinity@mail.ru
longdist.infinity@mail.ru
lucie.infinity@mail.ru
m4wl@list.ru
m8pwo@rambler.ru
makary.aaccf@mail.ru
marianne.aaccf@mail.ru
marin.aaccf@mail.ru
marta.aaccf@mail.ru
maryse.infinity@mail.ru
maury.aaccf@mail.ru
maxine.lamborgini@mail.ru
melony.octavia@mail.ru
mercie.aaccf@mail.ru
meriann.octavia@mail.ru
milt.octavia@mail.ru
minerva.aaccf@mail.ru
mlcc@mail.ru
mv2ttbb@yandex.ru
myx@spbcomail.ru
n@stmelf.bayern.de
nessa.aaccf@mail.ru
nigel.lamborgini@mail.ru
nikky.aaccf@mail.ru
noell.aaccf@mail.ru
novuzfypzyk@mail.ru
nwt7n@bk.ru
oldgakrutlojj@mail.ru
p9di@inbox.ru
puffiestk39@rambler.ru
pzmff@list.ru
qseadvo@yandex.ru
rantslla3@qip.ru
re@utilook.ru
reappliesic4@qip.ru
rededicatefx66@mail.ru
ru@spbedumail.ru
saz@reslist.ru
seajqj@bk.ru
sheliak34@qip.ru
sideburnse58@rambler.ru
silovnikita@bk.ru
spielingpyfc0@ya.ru
tmqaq9b@rambler.ru
uafv@inbox.ru
uf0rp@qip.ru
uq6gwx@rambler.ru
vuokcb@mail.ru
wbyfeem@inbox.ru
williemo@bk.ru
wotq9@mail.ru
xai20nu@qip.ru
xtts@rambler.ru
ybw1vgk@bk.ru
yzpmwmx@mail.ru
zwws@bk.ru

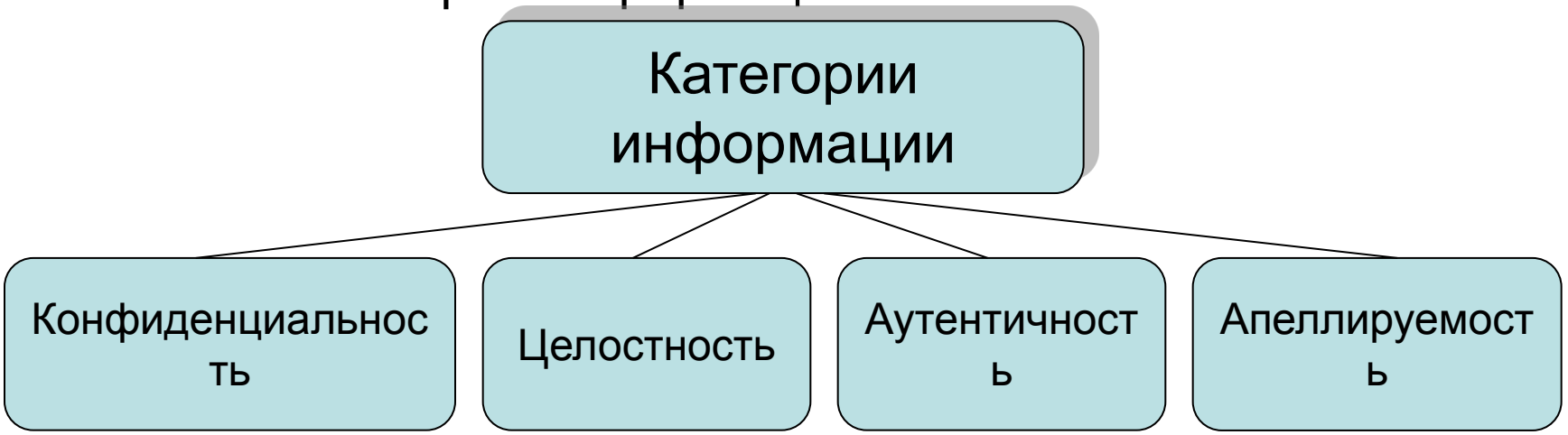
Текущие проблемы общества, связанные с информационной безопасностью

1. Обилие средств компьютеризации (от компьютеров и ноутбуков дома и на работе, заканчивая мобильными телефонами, аналогичными по функциям классическим компьютерам) при достаточно суровой степени ИТ-безграмотности пользователей.
2. Непонимание и неспособность защитить собственный труд и персональные данные, желание переложить ответственность на кого-то еще – провайдера, оператора связи, инженера, родственника и т.д.
3. Использование большой доли нелицензионного программного обеспечения, заражение своих компьютеров при «кряке», «взломе» и т.п.
4. Стремительное развитие информационных технологий зачастую делает невозможным вдумчивый анализ их известных и потенциальных уязвимостей. Большой объем «уязвимостей нулевого дня».

7 «грустных» принципов компьютерной безопасности

1. **Принцип пустого кармана**. «У меня нет ничего ценного, мне не надо защищаться».
2. **Принцип прививки**. «Однажды поставленный антивирус – защита».
3. **Принцип эгоиста**. «На своем компьютере я – единственный пользователь».
4. **Принцип лени.** «Мне так лениво вбивать каждый раз длинные имена и пароли, пусть всё подставляется автоматически»
5. **Принцип корзины яиц**. «Всё ценное лежит именно в моем компьютере и нигде больше».
6. **Принцип доверчивого ребенка**. «Всё, что пришло от моего друга – пришло от моего друга».
7. **Принцип склероза**. «Запишу, а то забуду»

Категории информационной безопасности



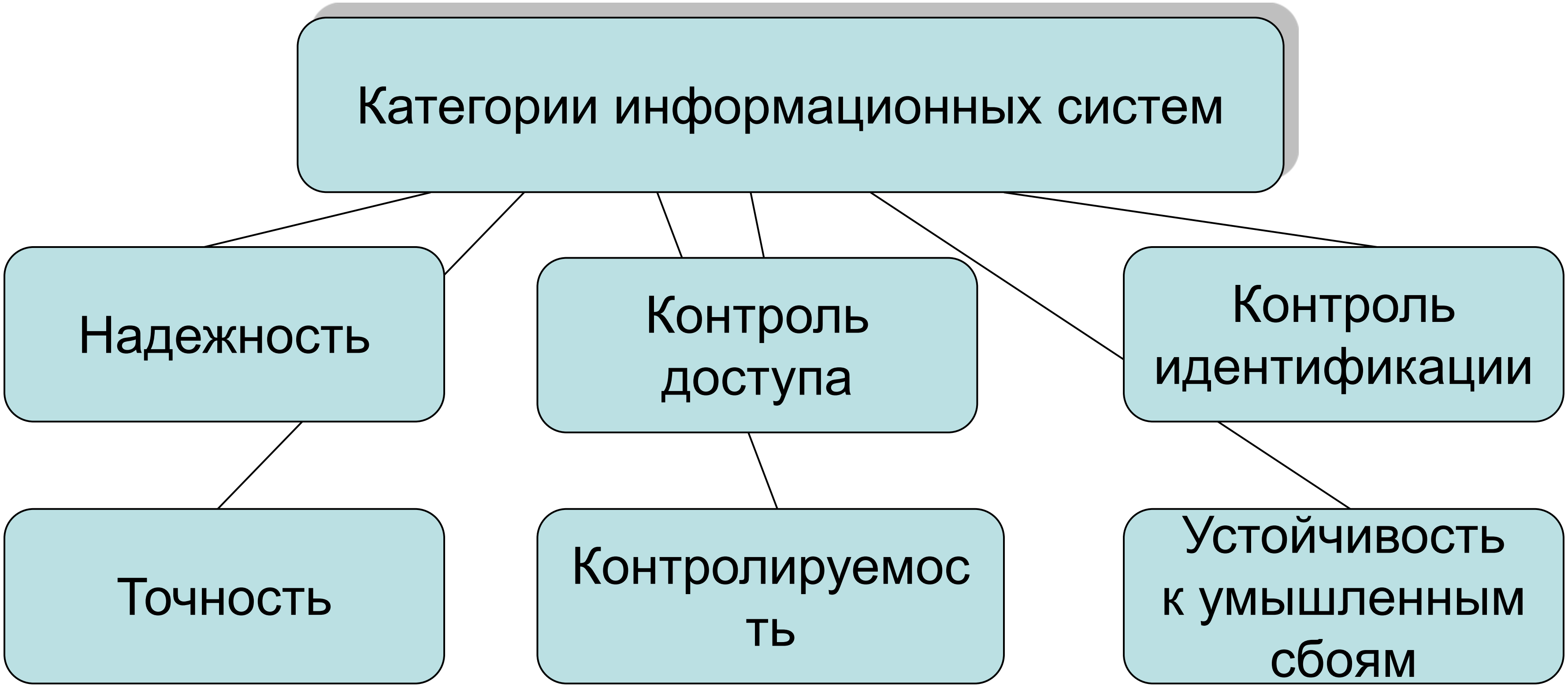
конфиденциальность – гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется ***хищением*** либо ***раскрытием информации***

целостность – гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется ***фальсификацией сообщения***

аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется ***фальсификацией***, но уже ***автора сообщения***

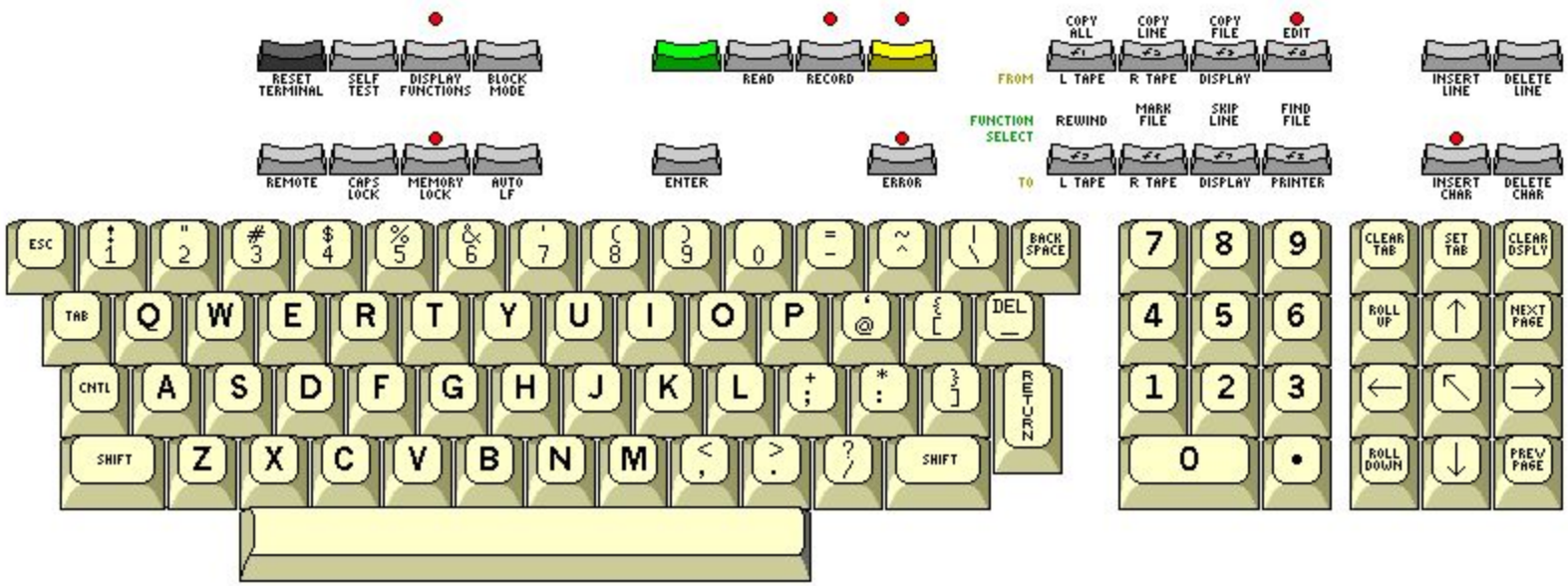
апеллируемость – гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой

Категории информационной безопасности



[illegible] …ения доступа постоянно выполняются

Терминалы защищенной информационной системы



Терминалы защищенной информационной системы

Требования использования терминалов с физическим доступом

1. Защищенность терминала должна соответствовать защищенности помещения;

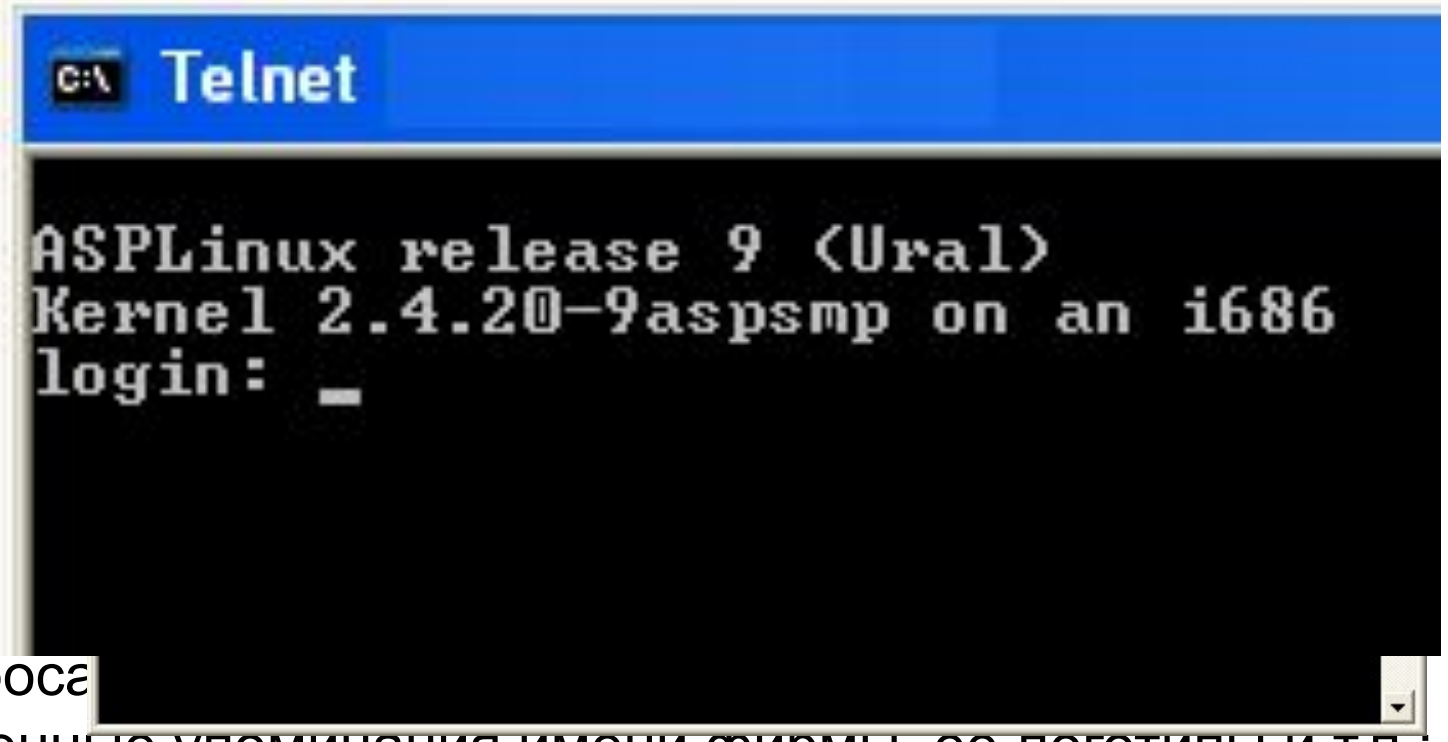
2. Системы контроля за доступом в помещение с установленным терминалом должны работать полноценно и в соответствии с общей схемой доступа к информации;

3. В случае установки терминала в местах с широким скоплением народа клавиатура, а если необходимо, то и дисплей должны быть оборудованы устройствами, позволяющими видеть их только работающему в данный момент клиенту.

Терминалы защищенной информационной системы

При использовании удаленных терминалов необходимо соблюдать следующие правила

1. Любой удале
   регистрации



2. Своевремен
   оборудовани
   не контролир

3. По возможно

4. Из log-in запроса
   непосредственные упоминания имени фирмы, ее логотипы и т.п.;

5. При входе в систему рекомендуется выводить на экран предупреждение о том, что вход в систему без таковых полномочий преследуется по закону.

Способы мошенничества в информационных системах

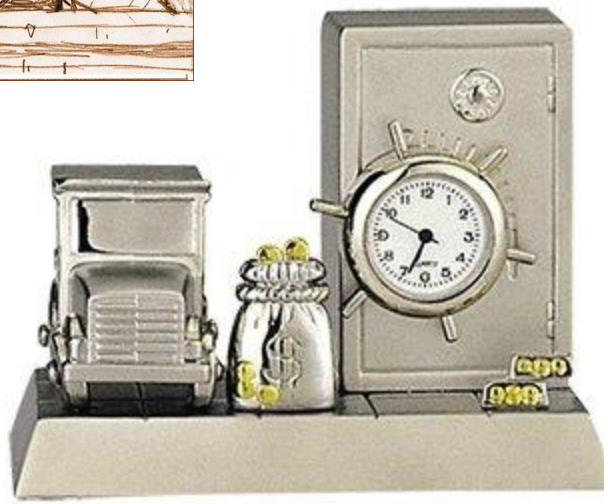
Способы мошенничества в информационных системах

Мошенничество (ст. 159 УК РФ) – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.

Компьютерные преступления (ст. 272, 273, 274 УК РФ) – неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшие уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. В соответствии с этими понятиями под способом мошенничества в ИС понимается совокупность приемов и средств, обеспечивших несанкционированный доступ к информационным ресурсам и технологиям и позволивших их противоправное использование.

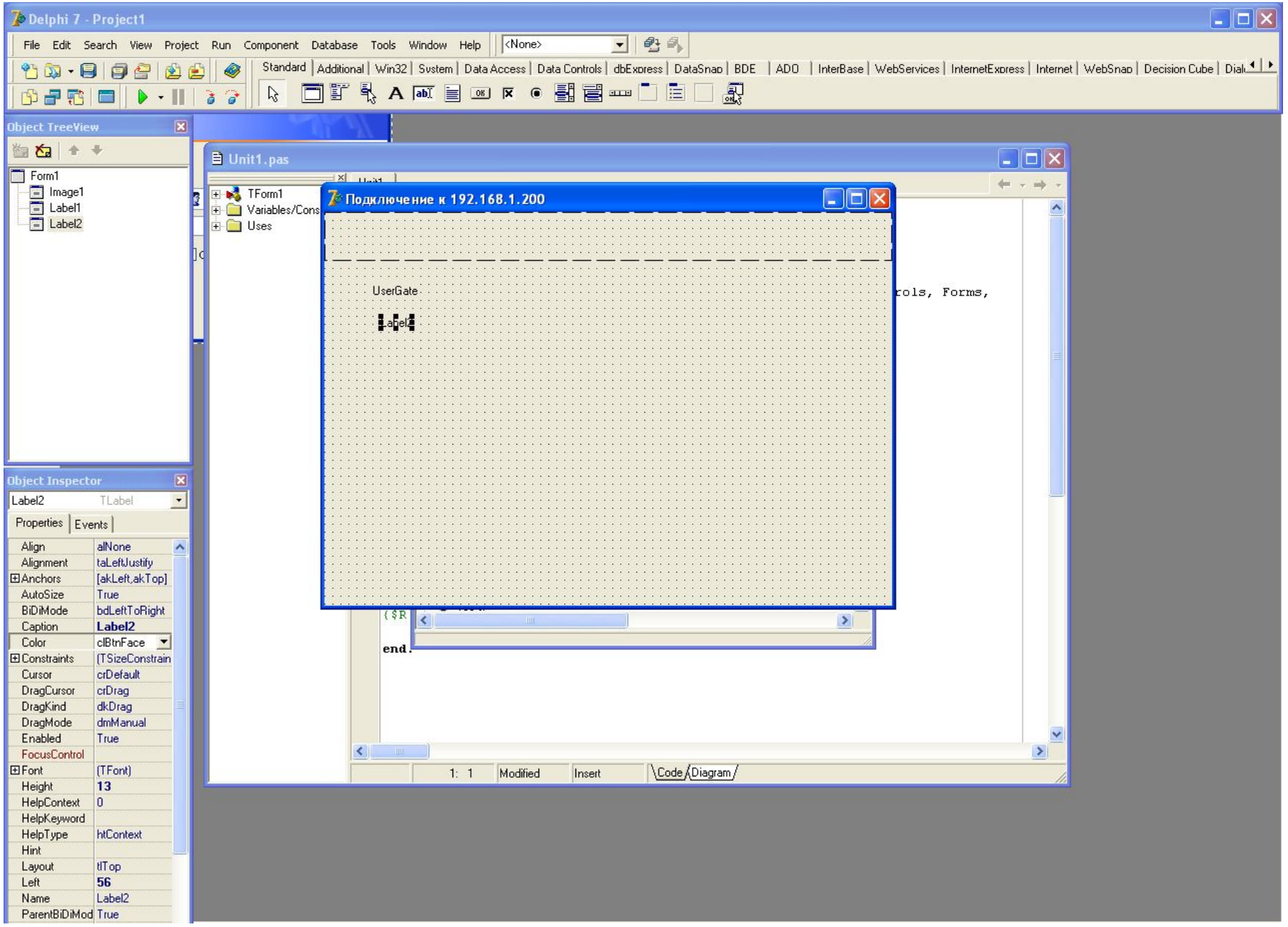
Способы мошенничества в информационных системах

1. Изъятие средств вычислительной техники
2. Перехват информации с использованием методов и аппаратуры аудио-, визуального и электромагнитного наблюдения
3. Несанкционированный доступ к СВТ, который реализуется с использованием следующих основных приемов:
   - «за дураком»
   - физическое проникновение
   - электронное проникновение
   - «за хвост»
   - «компьютерный абордаж»
   - «неспешный выбор»
   - «маскарад»
   - мистификация
   - «аварийный»
4. Способы бухгалтерского мошенничества:
   - «Салями»

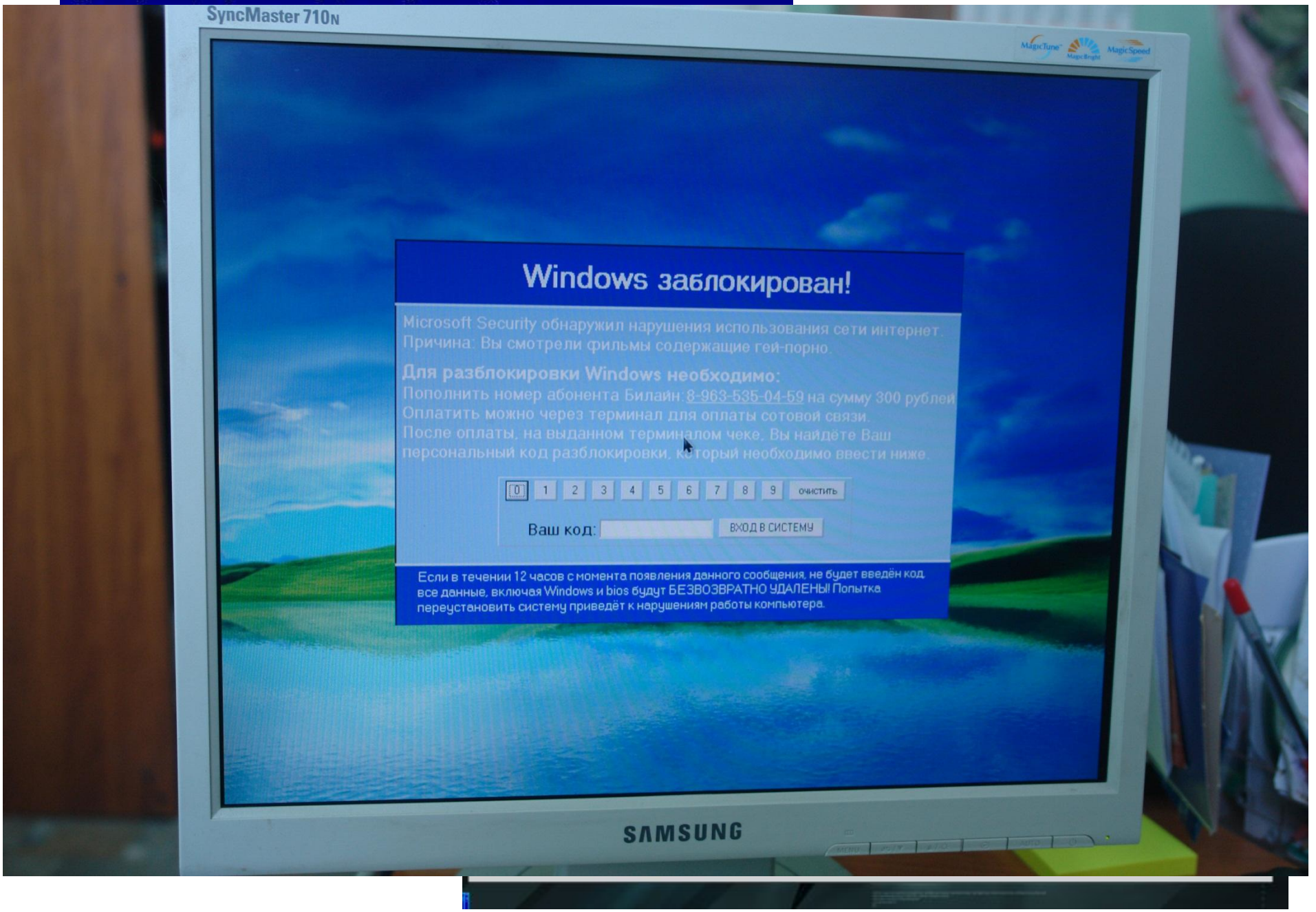


Сокрытие следов:

1. Дробление денежных сумм
2. Переброска денежных средств
3. «Бухинг»


Delphi 7 - Project1
File Edit Search View Project Run Component Database Tools Window Help
Standard Additional Win32 System Data Access Data Controls dbExpress DataSnap BDE ADO InterBase WebServices InternetExpress Internet WebSnap Decision Cube
Object TreeView
Form1
Image1
Label1
Label2
Object Inspector
Label2 TLabel
Properties Events
Align alNone
Alignment taLeftJustify
Anchors [akLeft,akTop]
AutoSize True
BiDiMode bdLeftToRight
Caption Label2
Color clBtnFace
Constraints (TSizeConstrain
Cursor crDefault
DragCursor crDrag
DragKind dkDrag
DragMode dmManual
Enabled True
FocusControl
Font (TFont)
Height 13
HelpContext 0
HelpKeyword
HelpType htContext
Hint
Layout tlTop
Left 56
Name Label2
ParentBiDiMod True
Unit1.pas
TForm1
Variables/Cons
Uses
Подключение к 192.168.1.200
UserGate
Label2
rols, Forms,
{$R
end.
1: 1
Modified
Insert
Code
Diagram

Мошенничество в сфере пластиковых карт - скиммеры


бнаружена проблема, которая может повредить вашему компьютеру.
SyncMaster 710N
Windows заблокирован!
Microsoft Security обнаружил нарушения использования сети интернет.
Причина: Вы смотрели фильмы содержащие гей-порно.
Для разблокировки Windows необходимо:
Пополнить номер абонента Билайн: 8-963-535-04-59 на сумму 300 рублей
Оплатить можно через терминал для оплаты сотовой связи.
После оплаты, на выданном терминалом чеке, Вы найдёте Ваш персональный код разблокировки, который необходимо ввести ниже.
0 1 2 3 4 5 6 7 8 9 очистить
Ваш код:
ВХОД В СИСТЕМУ
Если в течении 12 часов с момента появления данного сообщения, не будет введён код, все данные, включая Windows и bios будут БЕЗВОЗВРАТНО УДАЛЕНЫ! Попытка переустановить систему приведёт к нарушениям работы компьютера.
SAMSUNG

Социальная инженерия

Сообщение

23 апр 2009 в 3:53

От кого: Ольга Жукова

Кому: Юрий Quinto Преображенский

Тема: ...

Сообщение: Знаешь, мне на днях знакомый кинул ссылку на один сайт, там оказалась одна анкета с очень знакомым лицом...
Конечно увидеть тебя на таком сайте было неожиданностью, моё мнение о тебе изменилось...
Надеюсь ты понимаешь, что я имею в виду (http://erotok.net/2431/)
p.s не принимай близко у сердцу!

Закрыть | Это спам | Удалить

Ответить

[Показать всю историю сообщений]

Сообщение

9 мая 2009 в 16:26

От кого: Лёха Belyakop :-P Беляков

Кому: Юрий Quinto Преображенский

Тема: ...

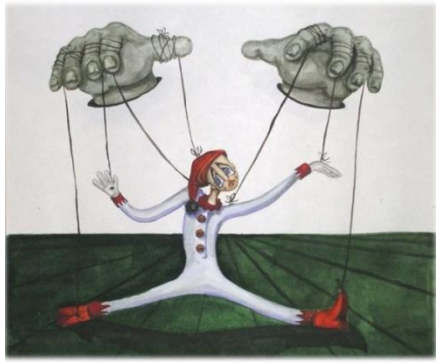
Сообщение: Привет.Как дела? Обращаюсь к тебе, т.к. знаю, что ты всегда поможешь..У меня мама учавствует в конкурсе,и пока на 2 месте. Можешь проголосватьза неё? отправить СМС,если конечно не жалко с текстом w8bb"пробел"b3576 на номер 3353 .Спасибо,думаю ты поймешь меня,для меня это очень важно.Как встретимся отблогадарю естесвенно.Юрий,Еще раз спасибо

Закрыть | Это спам | Удалить

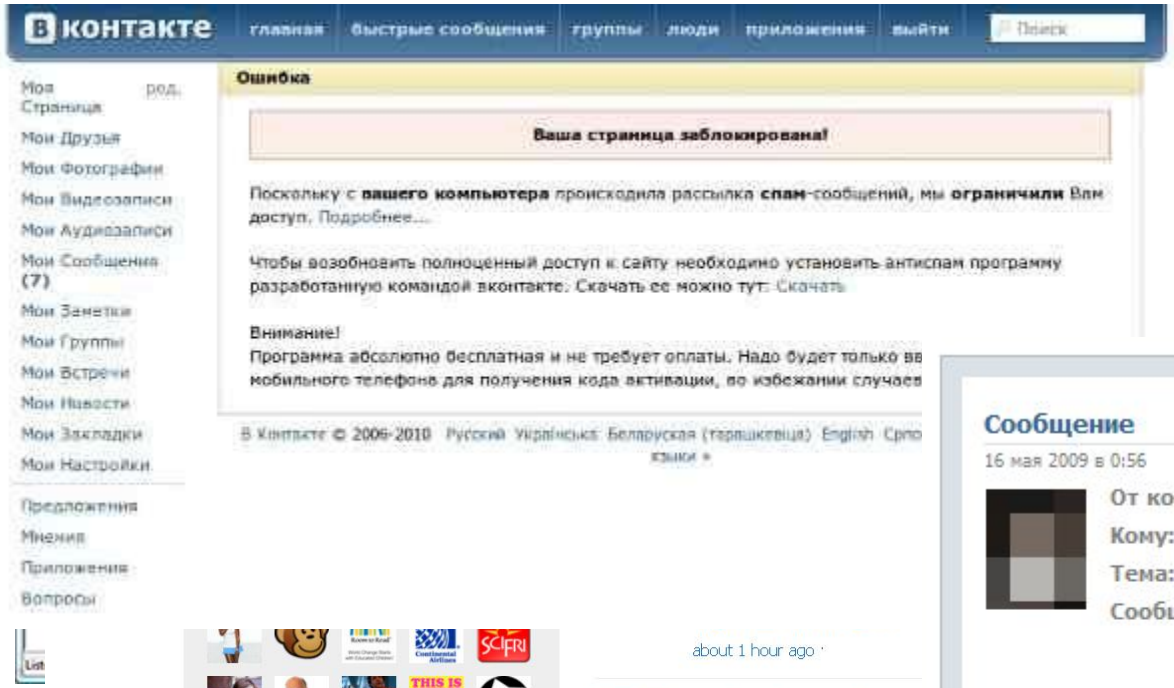
Ответить

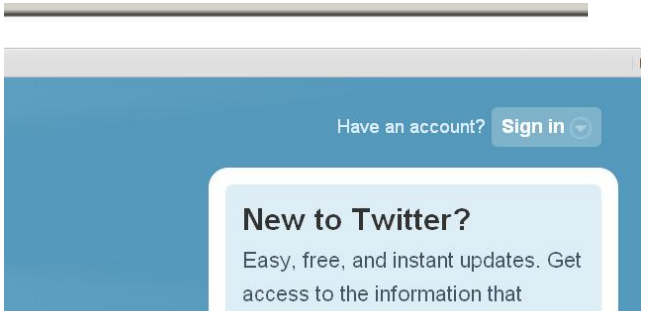
Пути мошенничества на базе социальной инженерии

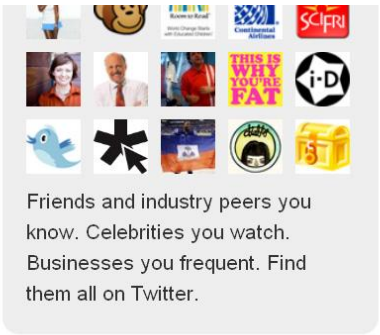
1. «Да, это стоит денег, но у нас –бесплатно»
2. «Вот документы, которые вы просили»
3. Претекстинг («У вас беда, но я вас спасу»)
4. Фишинг («Добро пожаловать, введите…»)
5. «Посмотри на этот клёвый файл»
6. Дорожное яблоко
7. «Я – ваш персональный инженер»

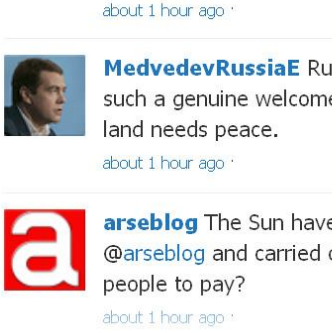


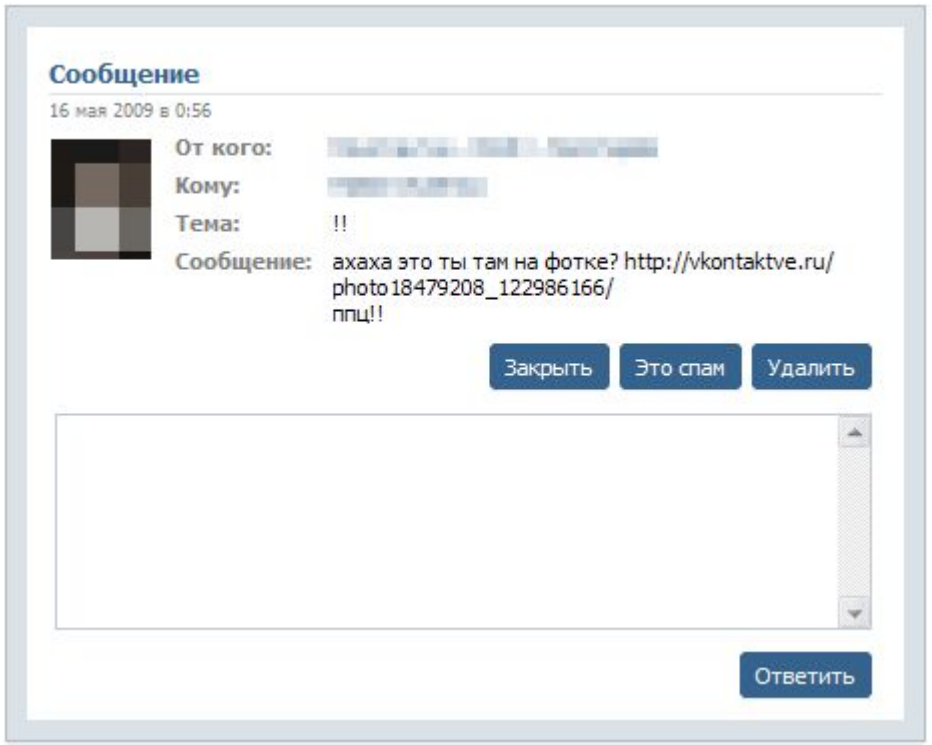
Фишинг: рыбалка и суровая проверка на внимательность





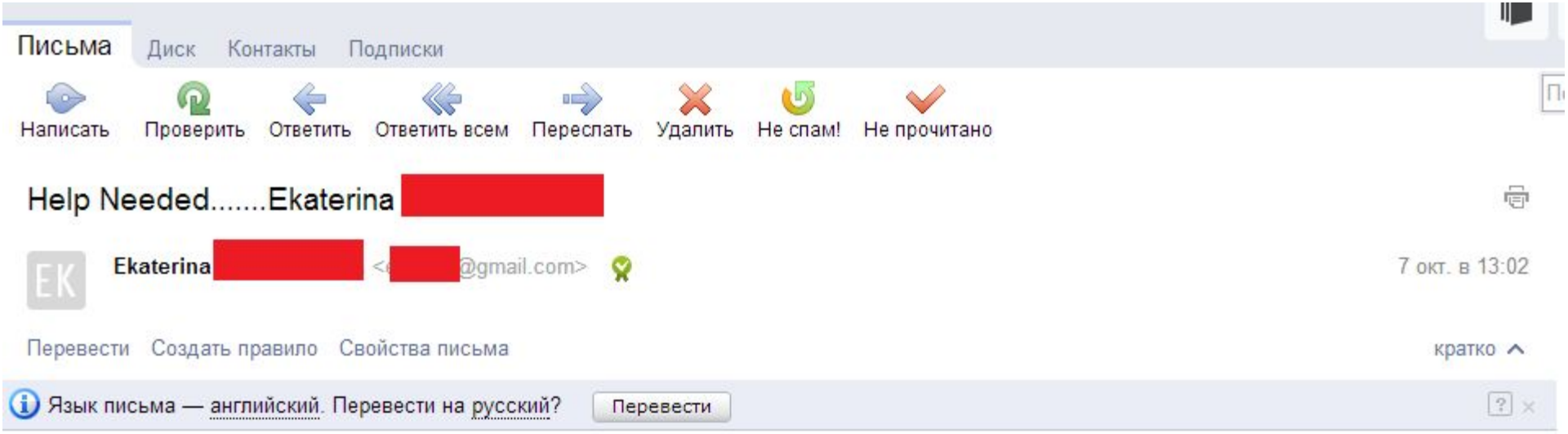






Один из методов фишинга: tabnabbing

1. Атакующий привлекает пользователя на страницу своего сайта, которая выглядит абсолютно нормальной и такой, какой пользователь ожидает её увидеть.
2. Атакующий определяет, что пользователь длительное время не взаимодействовал со страницей, или вообще переключился на другую вкладку.
3. Пока страница неактивна – подменяется ее favicon на иконку сайта, под который она будет маскироваться.
4. Контент страницы меняется на контент фейковой формы логина сайта, под который она маскируется.
5. С определенной достаточно большой долей вероятности пользователь, вернувшись ко вкладке – не задумываясь, автоматически введет свои логин и пароль.
6. После перехвата данных авторизации – пользователя можно просто переадресовать на атакуемый сайт, ведь вероятнее всего он на нем уже авторизован и именно этого поведения он и будет ожидать.



I'm writing this with tears in my eyes, My Family and I came to Philippines on a short holiday, unfortunately we got robbed at the park of the hotel were we Lodge, all cash, credit card and our mobile phone were stolen off. It was a bitter experience and we so luckily for us we still have our life and our passports safe.

We need your help flying back home as we are trying to raise some money.we have made contact with our bank but the best they can do is to mail me a new card which will take 2-3 days to arrive here.I need you to lend me some money to sort my self out of this predicament, will pay back once we get this over with.

Western Union Transfer is the fastest option to wire funds to me. Let me know if you need my details(Full names/location) to effect a transfer. You can reach me via email.I'm freaked out at the moment.

Thanks.
Ekaterina

MR Usman Pascal(ESQ)
Solicitors & Advocates
Block 7, Flat 8, Rue du Boulevard,
Lome-Togo
PB 37, +228 914 6970
Reply to usmanpascal77@gmail.com

Dear Preobrazhenskiy Yuriy,

On 23rd November by 3.30am GMT.time 2006, one of my clients named F.G.Preobrazhenskiy, a national of your country lost his life here as a result of lung cancer as confirmed by the medical specialist who was taking care of his illness for over three month before his death.

I have contacted you to ask your permission to present you to my late client's bank, so that some money (25.5)Twenty five million five hundred thousand united state dollar. he left behind by my client can be paid to your account as his beneficiary through my help and assistance, otherwise the money will be declared unserviceable by my late client's bank after 11 days. If you agree with me, i would prefer you send me your reply including your mobile phone number, so that i will call to give you more information.Pls kindly reply this mail to my chambers(usmanpascal77@gmail.com)
I am seriously waiting for your urgent reply
Thanks,
Usman Pascal
+228 914 6970
Email; usmanpascal77@gmail.com

FORM D2
ORIGINAL COPY
ENGLISH VERSION

REPUBLIQUE TOGOLAISE
COMMISSION NATIONALE DE LA POPULATION

Death Certificate

Issued under the Births and Deaths (Compulsory Registration) Decree 69 of 1982

D NO.: 769012

Registration Centre: CENTRALE HOSPITALIER DE TOKOIN

Town: LOME

Country: TOGO

Certification Number 83077

135 | 101 | 2007 CRD 572

Volume year Entry No

This is to certify that the death details of person whose picture appeared as recorded herein, has been registered on;

25TH (Day) DECEMBER (Month) 2003 (Year) at the Registration Centre

1. Full Name: PREOBRAZHENSKY YURICH OLEG
(Surname first) (in block letters)

2. Sex: MALE Country: RUSSIA

3. Date of Birth: 07 (Day) AUGUST (Month) 1948 (Year)

4. Age at Death: 55 YEARS

5. Cause of death: PLANE CRASH

6. Full Address of Usual place of residence of the Deceased: 11 AVENUE DU GENERALE DE GAULLE, FANITUA CONJI MUNICIPAL, LOME TOGO.

7. Place of Issue: CENTRALE HOSPITALIER LOME TOKOIN

8. Date of issue: 7TH JANUARY 2004

COMMISSION NATIONALE DE LA POPULATION TOGOLAISE LOME-TOGO

CHAIRMAN OF THE COMMISSION: DR. VAMIAGBO JACKO

REGISTRAR: MADAM AJOVI ESOCH

Некоторые примеры грязной и не очень грязной социальной инженерии

Приветик..!!))

Анфисочка Страхова [t-higa@group.omotokai.jp]

Ссылки и другие функциональные возможности в этом сообщении отключены. Чтобы восстановить эти функции, переместите сообщение в папку "Входящие".
Дополнительные разрывы строк в сообщении были удалены.

Отправлено: Вт 20.12.2011 2:46
Кому: [redacted]

твой email адресс ммне дала Лилька..
меня она попросила кинуть тебе на этот сайт ссылку http://vliegticketsinfo.nl/video.php
она сказала, что это чтото офигенное и тебе будет интересно..!!) любопытства ради я и сама открыла ссылку..!)) и это оказалось архив с фильмами..... очень класно. теперь сижу и смотрю.!))

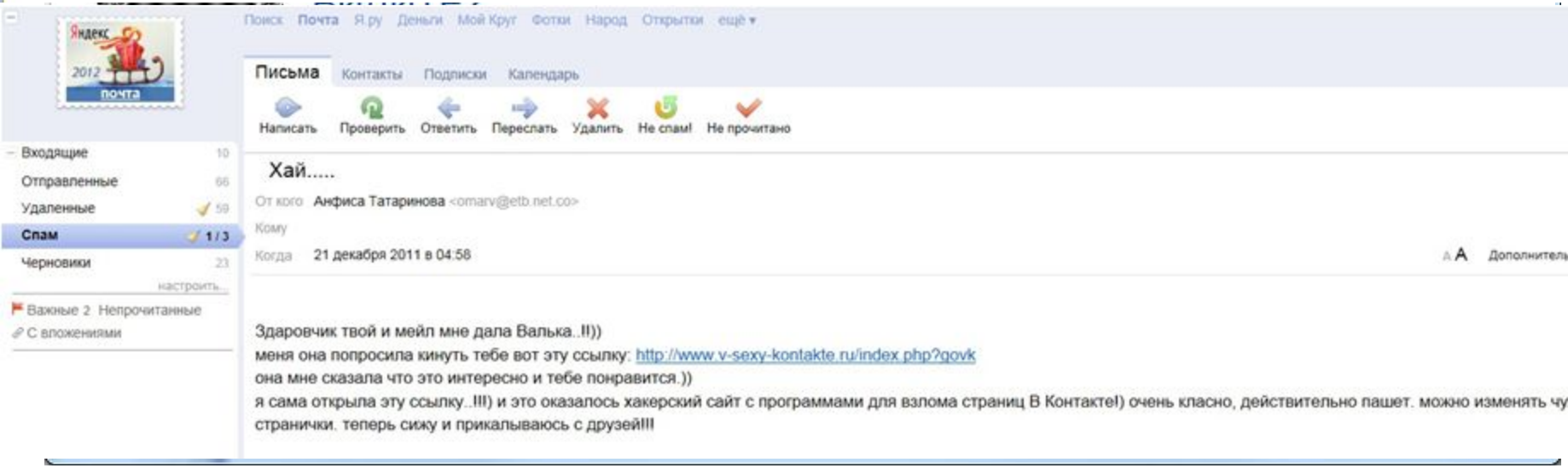
Трямс, милый .)

Евгения Андрейченко [info@wombmusic.net]

Ссылки и другие функциональные возможности в этом сообщении отключены. Чтобы восстановить эти функции, переместите сообщение в папку "Входящие".
Дополнительные разрывы строк в сообщении были удалены.

Отправлено: Сб 17.12.2011 19:31
Кому: [redacted]

Здаров твой адрес дала Янка..)
а ты красивый, .!!)
Ищу как бы отношения с как бы парнем.. но без обязательств в принципе только секс..
если хош зазнакомиться, заходь ко мне на страничку!!!) сижу на этом сайтичке http://fre3.ru/esd/index.php - пиши, я включу вебку!))) ТОЛЬКО БЕЗ ОБИД.!)))



Я СЕГОДНЯ ПРЕБЫВАЮ В ШОКОВОМ СОСТОЯНИИ!

aldoavoto

Письма | Контакты | Подписки | Календарь

Написать | Проверить | Ответить | Переслать | Удалить | Не спам! | Не прочитано

Найти | Переложить в папк | пред. след.

Яндекс.Подарки - не упусти свой шанс!

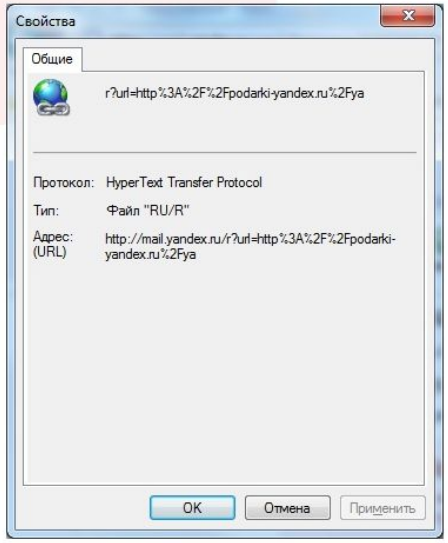
От кого nick@sw-fans.net
Кому @yandex.ru
Когда 27 января 2012 в 16:33

A A Дополнительно

Яндекс.Почта считает это письмо мошенническим

Не отвечайте на него и не совершайте никаких действий, описанных в тексте.
Рекомендуем удалить это письмо.

Удалить это письмо



Яндекс.Подарки

Получи свой подарок от нового сервиса Яндекс.Подарки.
Наша компания поздравляет своих пользователей и дарит всем прекрасные подарки.
Что бы получить свой подарок посетите Яндекс прямо сейчас!

С уважением администрация Яндекс.

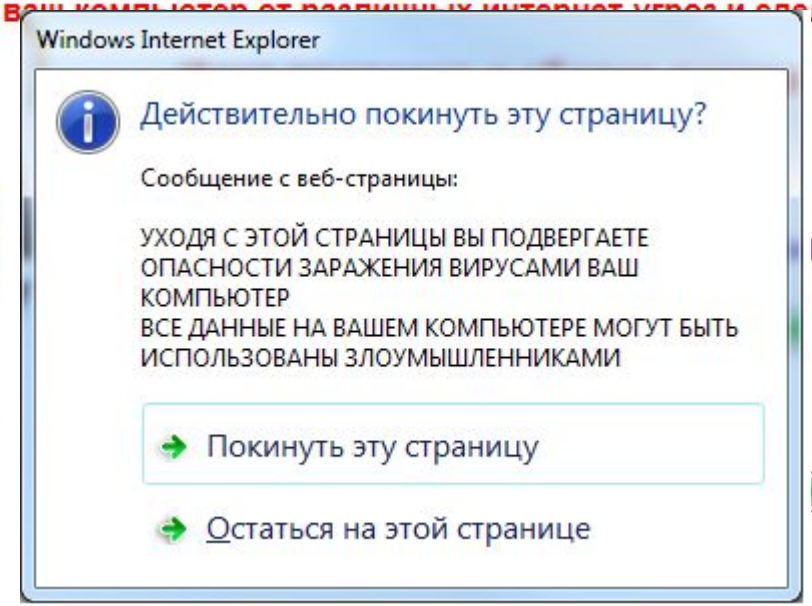
Ответить | Ответить всем | Переслать | Удалить

Напишите ответ здесь

POST.AMBN

Internet Explorer Обновление Вашего браузера

Внимание!!! Ваш браузер устарел! Настоятельно рекомендуем обновить его!
Новая версия браузера защитит ваш компьютер от различных интернет угроз и сделает его более безопасным.



овлений для

Активировать

Парольная защита

«Что такое брелок? Это такая штуковина, позволяющая потерять все ключи сразу» (Народная мудрость)

Один пароль «на всё» равнозначен замку, который открывается согнутым гвоздем (еще одна народная мудрость)

Примеры отвратительных паролей

1 1234

qwerty q1w2e3r4t5y6

12031973 12031973

89102401122 205634

lena petrova

microsoft secret

gfhjkm ctrhtn

Примеры хороших паролей

Qla0Ti56C0

Dfhjybi2004 *(Вароniш2004)*

B1df1yj1dB1df1y (И1ва1но1вИ1ва1н)

Nhtym<htymYANDEX(ТреньБреньYANDEX)

Рекомендуемый набор паролей

1 пароль – «мастер-пароль»	Электронная почта
2 пароль – коммуникационный пароль	ICQ, Skype
3 пароль –«хорошие ресурсы»	Чаты, форумы, подписки…
4 пароль – «нехорошие ресурсы»	
5 пароль – платежный пароль	Webmoney, Яндекс.Деньги

Основные требования информационной безопасности к методу парольной защиты

1. Вход всех пользователей в систему должен подтверждаться вводом уникального для клиента пароля.
2. Пароль должен тщательно подбираться так, чтобы его информационная емкость соответствовала времени полного перебора пароля.
3. Пароли по умолчанию должны быть сменены до официального запуска системы и даже до сколь либо публичных испытаний программного комплекса.
4. Все ошибочные попытки войти в систему должны учитываться, записываться в файл журнала событий и анализироваться через "разумный" промежуток времени.
5. В момент отправки пакета подтверждения или отвержения пароля в системе должна быть установлена разумная задержка.

Основные требования информационной безопасности к методу парольной защиты

6. Все действительные в системе пароли желательно проверять современными программами подбора паролей, либо оценивать лично администратору системы.
7. Через определенные промежутки времени необходима принудительная смена пароля у клиентов.
8. Все неиспользуемые в течение долгого времени имена регистрации должны переводиться в закрытое (недоступное для регистрации) состояние. Это относится к сотрудникам, находящимся в отпуске, на больничном, в командировке, а также к именам регистрации, созданным для тестов, испытаний системы и т.п.
9. От сотрудников и всех операторов терминала необходимо требовать строгое неразглашение паролей, отсутствие каких-либо взаимосвязей пароля с широкоизвестными фактами и данными, и отсутствие бумажных записей пароля "из-за плохой памяти".

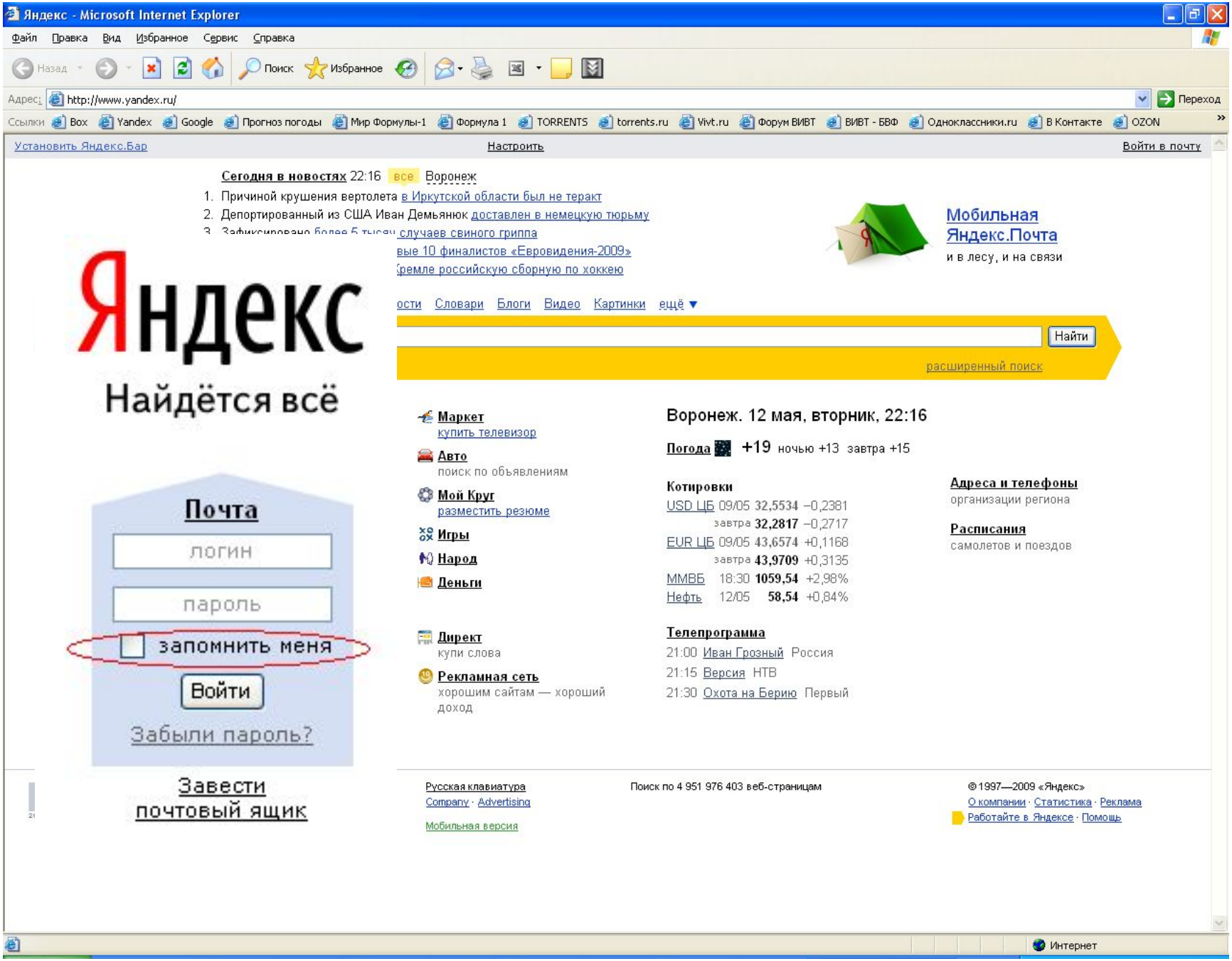
Формула для расчета числа попыток входа в систему

Число попыток входа:

K=max(int(N*0.1*3)+1, 3)

0.1 – 10% порог «забывчивости»

3 – стандартное число попыток


Яндекс - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
Назад Поиск Избранное
Адрес: http://www.yandex.ru/
Переход
Ссылки Box Yandex Google Прогноз погоды Мир Формулы-1 Формула 1 TORRENTS torrents.ru Vivt.ru Форум ВИВТ ВИВТ - ВВФ Одноклассники.ru В Контакте OZON
Установить Яндекс.Бар
Настроить
Войти в почту
Сегодня в новостях 22:16 все Воронеж
1. Причиной крушения вертолета в Иркутской области был не теракт
2. Депортированный из США Иван Демьянюк доставлен в немецкую тюрьму
случаев свиного гриппа
вые 10 финалистов «Евровидения-2009»
Кремле российскую сборную по хоккею
Мобильная Яндекс.Почта
и в лесу, и на связи
Яндекс
Найдётся всё
ости Словари Блоги Видео Картинки ещё
Найти
расширенный поиск
Маркет
купить телевизор
Авто
поиск по объявлениям
Мой Круг
разместить резюме
Игры
Народ
Деньги
Директ
купи слова
Рекламная сеть
хорошим сайтам — хороший доход
Воронеж. 12 мая, вторник, 22:16
Погода +19 ночью +13 завтра +15
Котировки
USD ЦБ 09/05 32,5534 −0,2381
завтра 32,2817 −0,2717
EUR ЦБ 09/05 43,6574 +0,1168
завтра 43,9709 +0,3135
ММВБ 18:30 1059,54 +2,98%
Нефть 12/05 58,54 +0,84%
Адреса и телефоны
организации региона
Расписания
самолетов и поездов
Телепрограмма
21:00 Иван Грозный Россия
21:15 Версия НТВ
21:30 Охота на Берию Первый
Почта
логин
пароль
запомнить меня
Войти
Забыли пароль?
Завести почтовый ящик
Русская клавиатура
Company · Advertising
Мобильная версия
Поиск по 4 951 976 403 веб-страницам
©1997—2009 «Яндекс»
О компании · Статистика · Реклама
Работайте в Яндексе · Помощь
Интернет

@MAIL.RU: почта, новости, работа, рассылки, развлечения. Почта @MAIL.RU - бесплатная почта #1 - Microsoft Internet Explorer

Файл Правка Вид Избранное Сервис Справка

Назад Поиск Избранное

Адрес: http://www.mail.ru/ Переход

Ссылки Box Yandex Google Прогноз погоды Мир Формулы-1 Формула 1 TORRENTS torrents.ru Vivt.ru Форум ВИВТ ВИВТ - БВФ Одноклассники.ru В Контакте OZON

Internet Explorer 8 Internet Explorer 8 с сервисами от Mail.Ru. Доступен уже сегодня! Скачать

@mail.ru национальная почтовая служба

Поиск в Интернете Например: почему слоны не летают Найти

ры Софт Словари Карты new

почта агент

Регистрация в почте

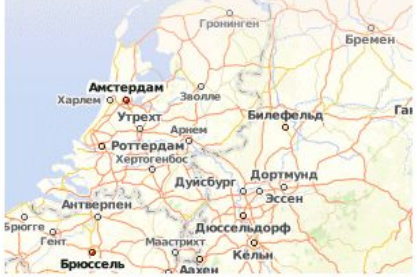
Имя @mail.ru

Пароль Забыли?

Чужой компьютер Войти

проводе

ОБЗОРНАЯ КАРТА МИРА



Работа Софт
Путешествия Ответы
Леди Чаты
Дети Шоубиз
Недвижимость Товары

+19°
ночью: +14°
завтра: +12°
ясно

$ 32.2817 −0.2717
€ 43.9709 +0.3135

21:30 Охота на Берию
21:00 Иван Грозный
21:15 Версия

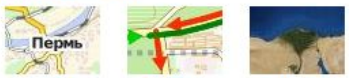
Фото и Видео

Товары Конкурс! Барахолка new

Коллекция лучших видеоклипов:
Поп, Рок, Рэп, Саундтреки и многое другое. Смотри на Видео@Mail.Ru

Звездные блоги

Карты@Mail.Ru



карты пробки спутники

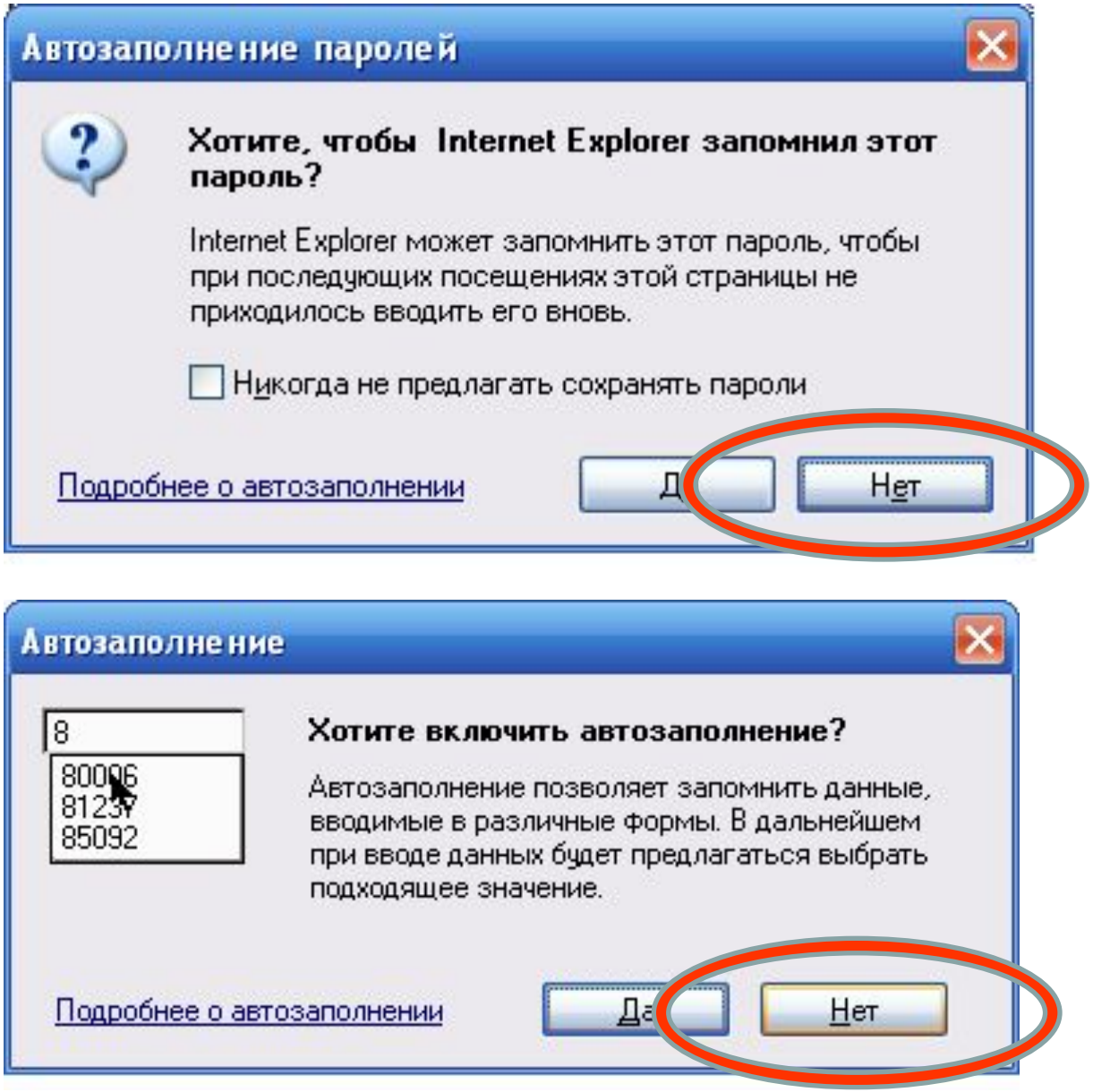
Каталог сайтов | Каталог сообществ

- Непознанное, Гороскопы
- Культура и искусство
- Наука и образование
- Майские каникулы
- Новости и Справки
- Отдых, Туризм, Юмор
- Общество и политика
- Товары и услуги, Авто
- Бизнес и финансы
- Производство и Работа
- Компьютеры и Интернет
- Домашний очаг, Медицина
- Недвижимость, Спорт
- ЧМ-2009 по хоккею

Мини-игры

Шахматы Косможестянка Бомберы Шарики

Готово Интернет


Автозаполнение паролей
Хотите, чтобы Internet Explorer запомнил этот пароль?
Internet Explorer может запомнить этот пароль, чтобы при последующих посещениях этой страницы не приходилось вводить его вновь.
Никогда не предлагать сохранять пароли
Подробнее о автозаполнении
Нет
Автозаполнение
8
80096
81237
85092
Хотите включить автозаполнение?
Автозаполнение позволяет запомнить данные, вводимые в различные формы. В дальнейшем при вводе данных будет предлагаться выбрать подходящее значение.
Подробнее о автозаполнении
Нет

Получение паролей на основе ошибок в реализации

Атака на хранилище паролей

Использование недокументированных возможностей системы

Перехват ввода с клавиатуры

Работа программы-перехватчика

Адекватная защита от запуска сторонних программ
Система единовременных паролей

Перехват при передаче по сети

Протоколы передачи
Модификация сетевого программно-аппаратного обеспечения

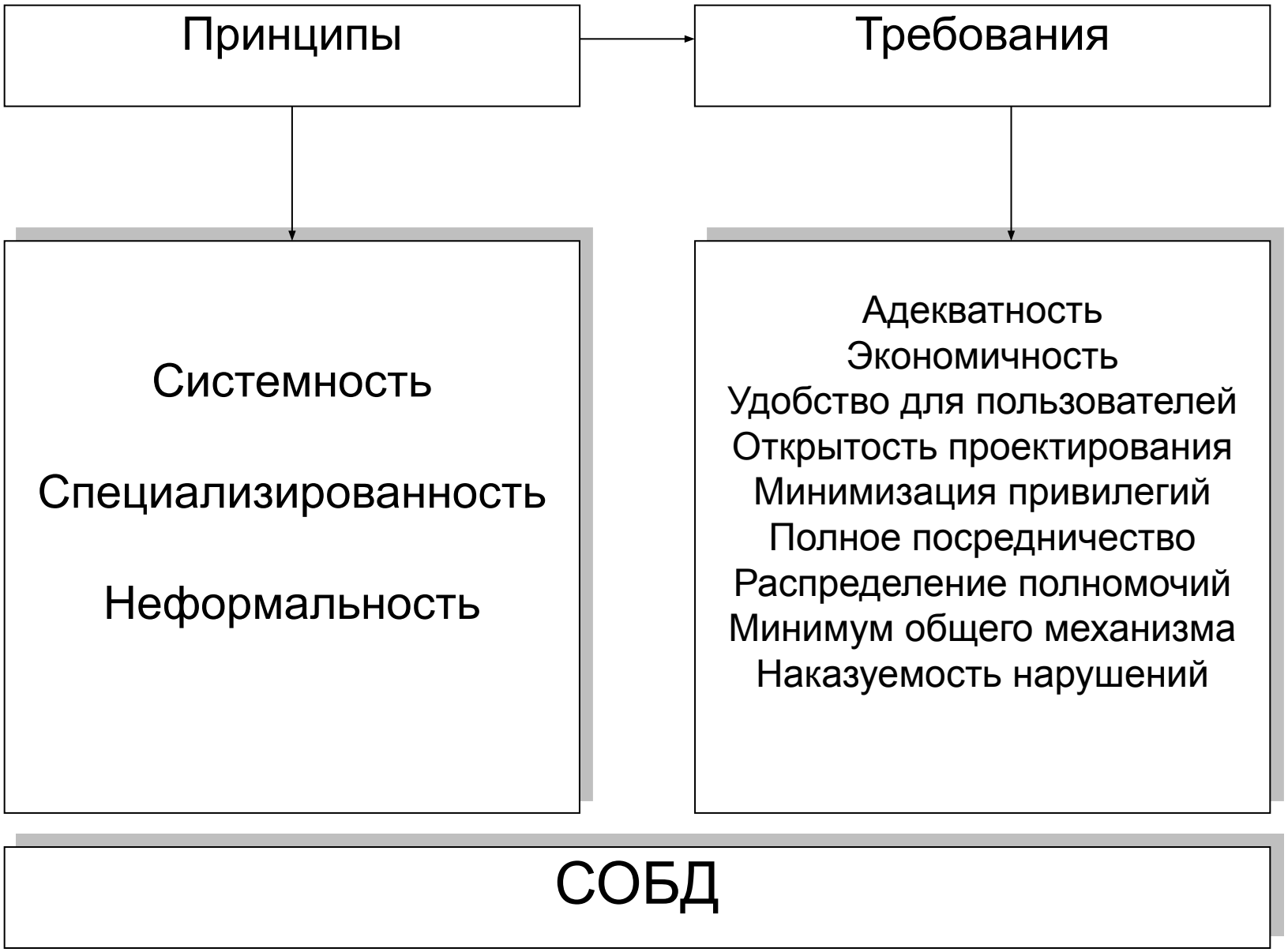
Ограничение физического доступа к кабелям
Избегание использования широковещательных топологий
Защита как внутреннего, так и внешнего трафика

Цели и задачи защиты информации в ИВС

Принципы и требования к системе безопасности данных

Цель и задачи защиты данных в ИВС

Принципы организации систем обеспечения безопасности данных (СОБД) ИВС

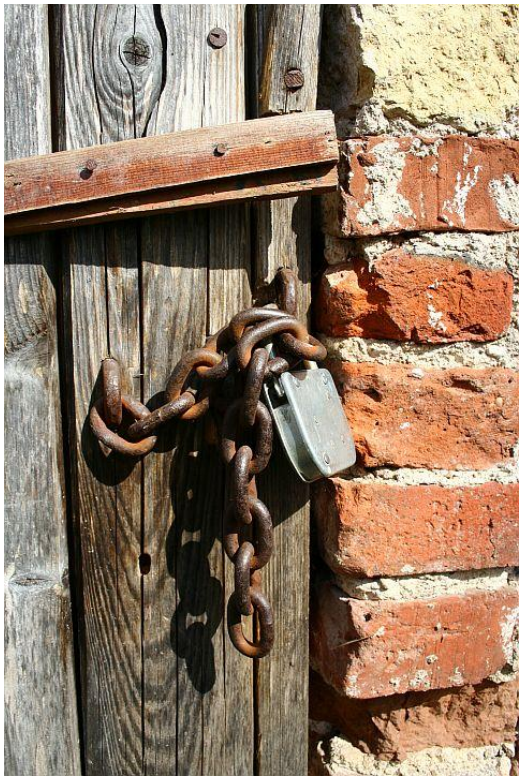


Раздел второй

«Методы и средства защиты данных»

Классификация средств защиты данных

Физические средства защиты



Физические средства защиты

Физические средства защиты выполняют следующие основные функции:

– охрана территории и зданий;

– охрана внутренних помещений;

– охрана оборудования и наблюдение за ним;

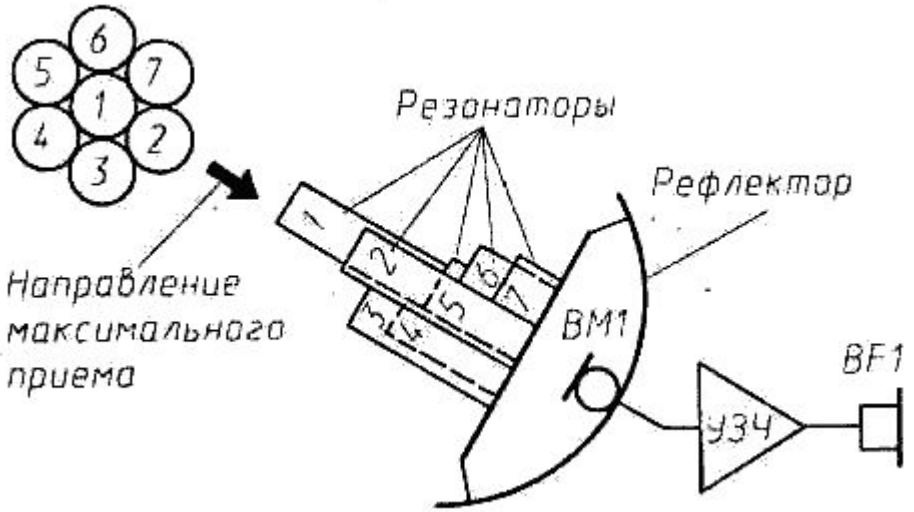
– контроль доступа в защищаемые зоны;

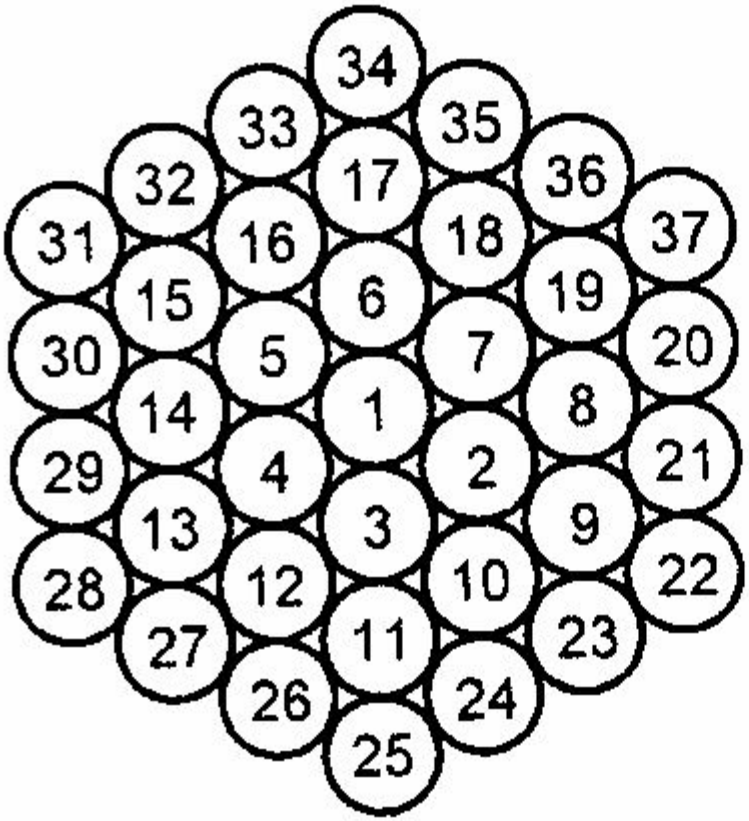
– нейтрализация излучений и наводок;

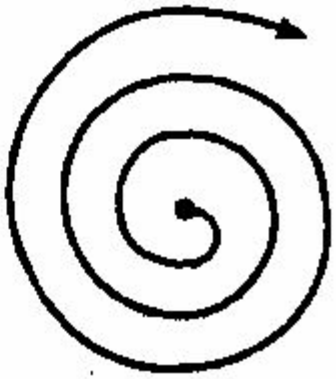
– создание препятствий визуальному наблюдению и подслушиванию;

– противопожарная защита;

– блокировка действий нарушителя

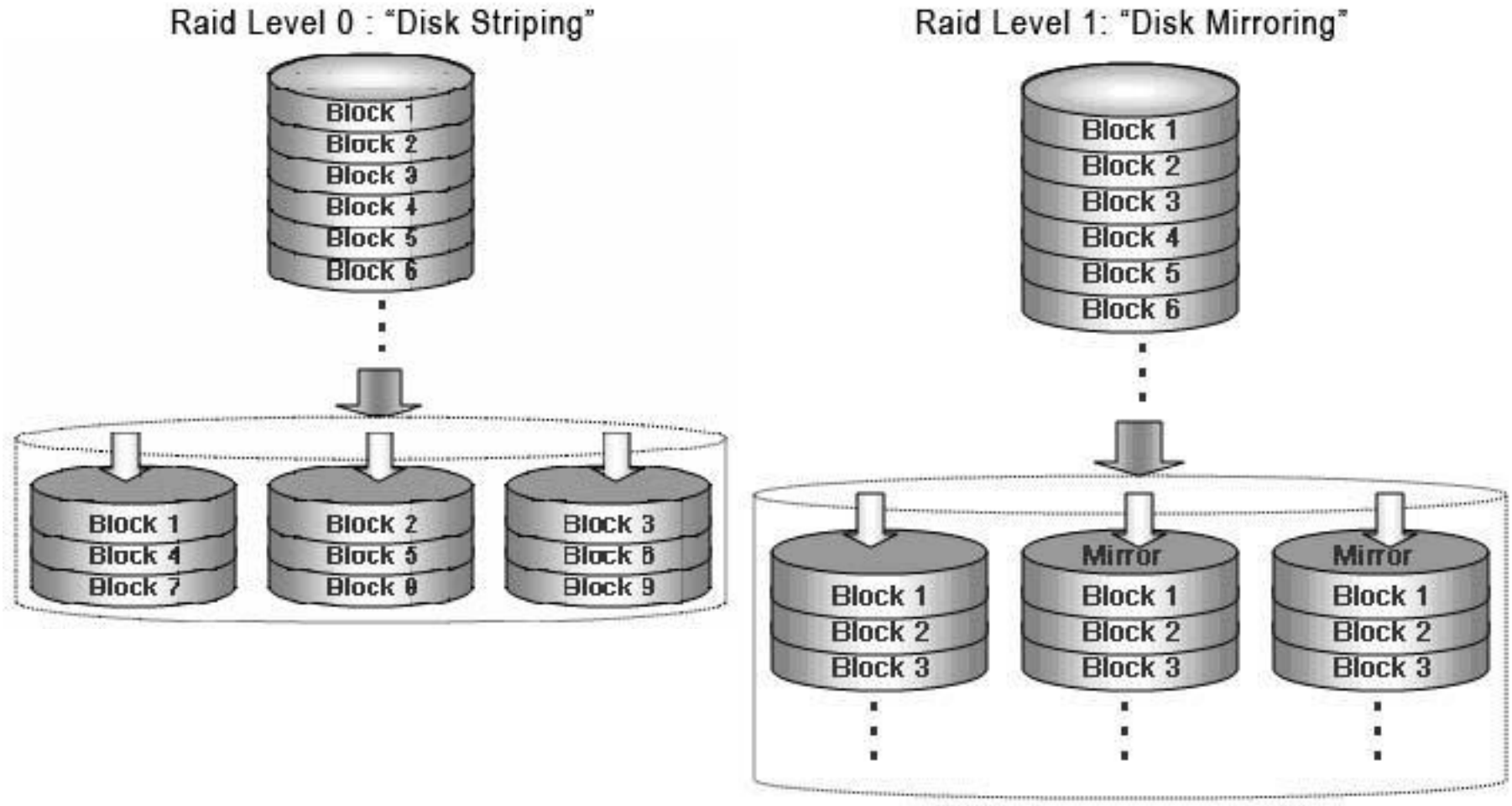

6
5
7
1
4
2
3
Резонаторы
Рефлектор
Направление максимального приема
BM1
BF1
УЗЧ


34
33
35
32
17
36
31
16
18
37
15
6
19
30
5
7
20
14
1
8
29
4
2
21
13
3
9
28
12
10
22
27
11
23
26
24
25

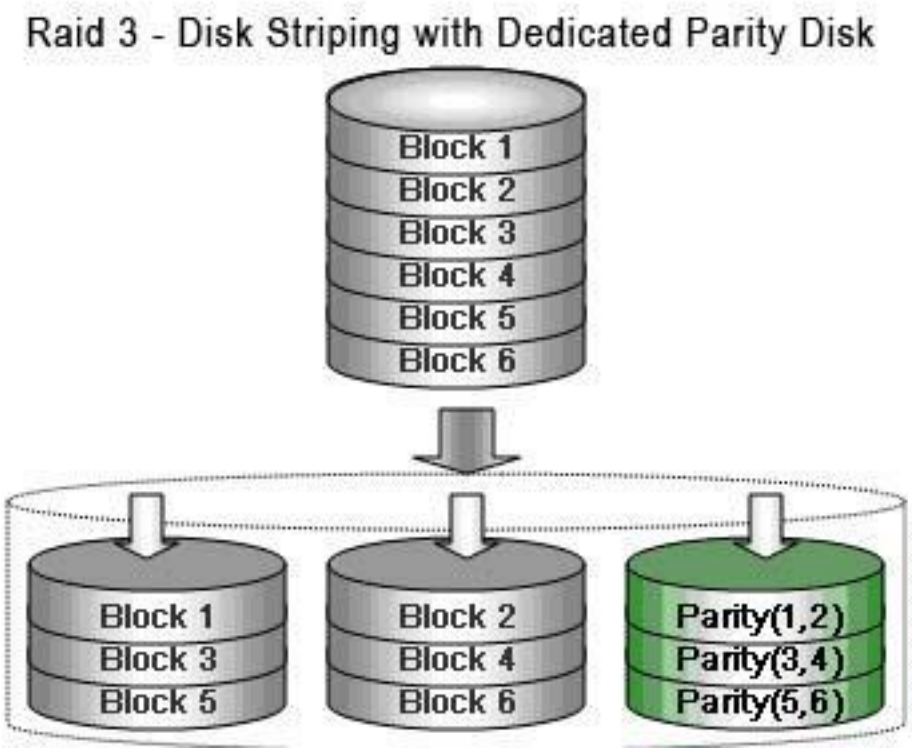


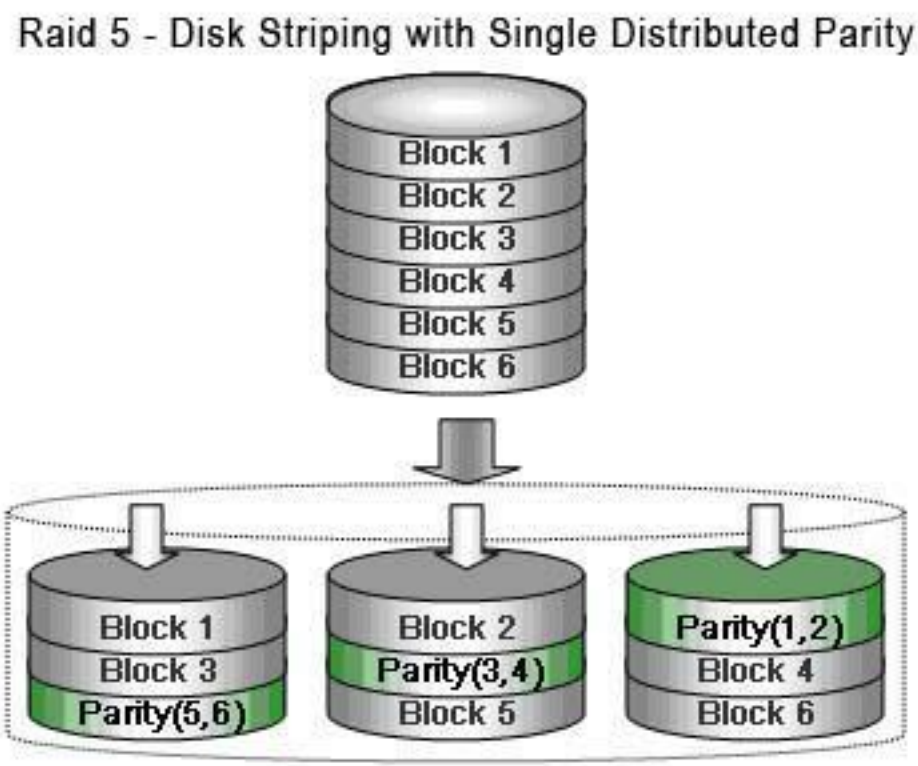
Аппаратные средства защиты

RAID −Redundant Array of Independent Disks (Избыточный массив независимых дисков)



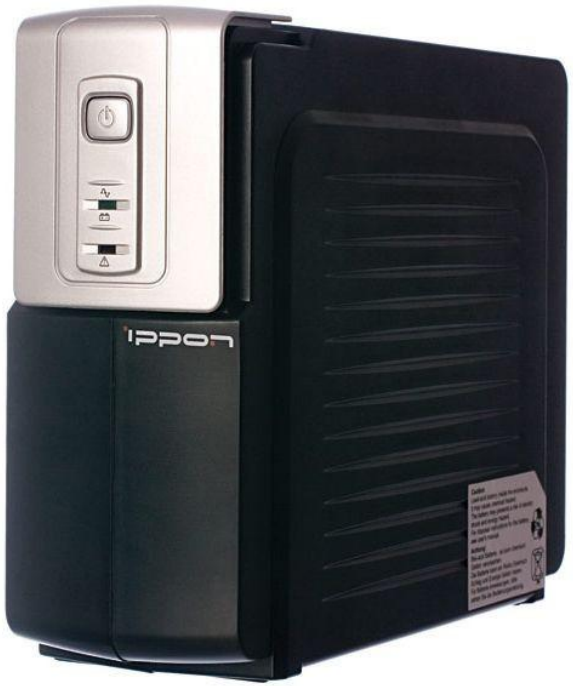
Аппаратные средства защиты



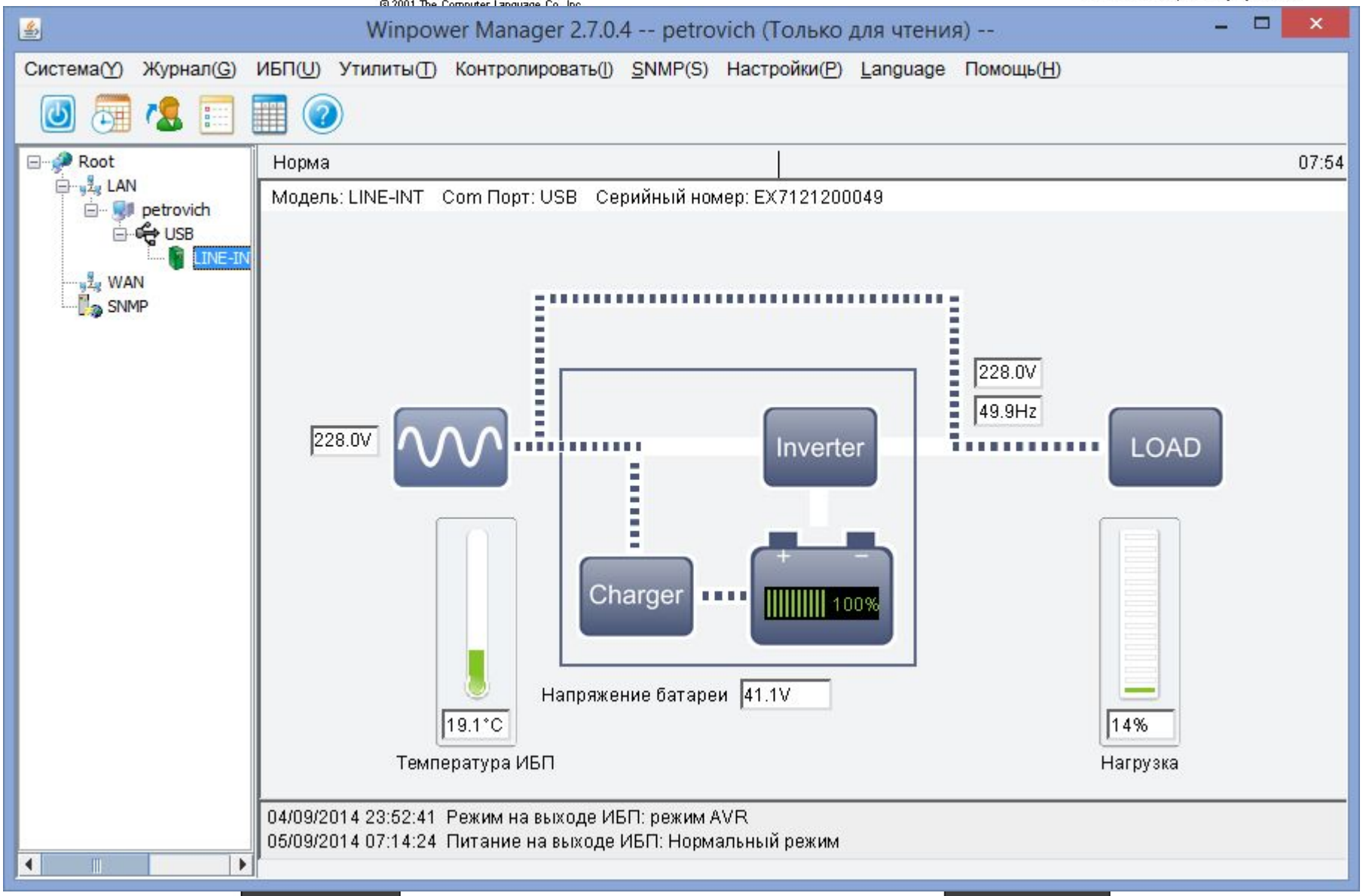


Аппаратные средства защиты

UPS – Uninterruptible Power Supply
(Источник бесперебойного питания)



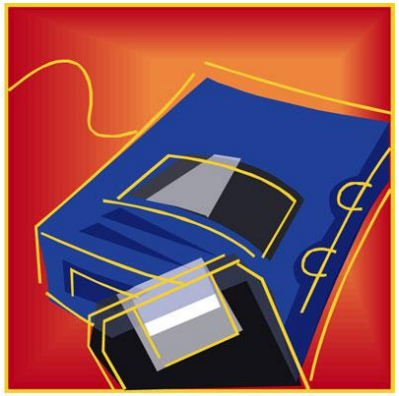
Аппаратные средства защиты

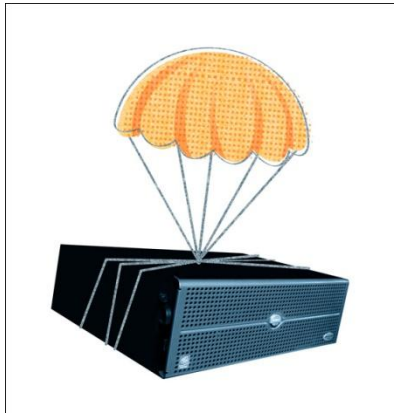


Аппаратные средства защиты

	Высоко-вольтные выбросы (Spikes)	**Высоко-частотный шум (Line Noise)**	**Подсадка напряжения (Brownout)**	**Исчезновение напряжения (Blackout)**
Сетевые фильтры	Частично	Нет	Нет	Нет
Стабилизаторы	Да	Частично	Частично	Нет
ИБП Off-Line	Нет	Частично	Частично	Да
ИБП Line-Interactive	Нет	Частично	Частично	Да
ИБП On-Line	Да	Да	Да	Да

Резервирование данных





- Классификация
- резервирования
  - Полное
  - резервирование

  - Инкрементное
  - резервирование

  - Дифференциальное
  - резервирование


ДИФФЕРЕНЦИАЛЬНОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ
2
Резервируемые данные
операционная система
программы пользователя
данные
A
B
C
4
Резервируемые данные
измененные файлы
C
новые файлы
D
7
Резервируемые данные
C
D
измененные файлы
A
новые файлы
E
ИНКРЕМЕНТНОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ
2
Резервируемые данные
операционная система
программы пользователя
данные
A
B
C
4
Резервируемые данные
измененные файлы
C
новые файлы
D
7
Резервируемые данные
измененные файлы
A
новые файлы
E

Циклы использования носителей для резервирования

	Day of the Cycle							
	1	2	3	4	5	6	7	8
Set	A		A		A		A	
		B				B		
				C				C

Four-Tape Hanoi Schedule

	Day of the Cycle															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Set	A		A		A		A		A		A		A		A	
		B				B				B				B		
				C								C				
								D								D

Five-Tape Hanoi Schedule

	Day of the Cycle																													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Set	A		A		A		A		A		A		A		A		A		A		A		A		A		A		A		A	
		B				B				B				B				B				B				B				B		
				C								C								C								C				
								D																D							
																E															E

Сменные носители для резервирования информации

Носитель	Объем, Мб	Цена, руб.				
FD		20↑				
CD-R		8				
CD-RW		15				
DVD-R		11				
DVD-R		25				
DVD-DL		50				
Blu-Ray		100↓				
Flash		600↓				
Стример	260 000	1103→	+	184 000	1..2	0..1→

Цена за 1Гб: 14628р.

Цена за 1Гб: 12р.

Цена за 1Гб: 21р.

Цена за 1Гб: 2р.

Цена за 1Гб: [illegible]

Цена за 1Гб: [illegible]

Цена за 1Гб: 4р.

Цена за 1Гб: [illegible]

Цена за 1Гб: 4р. – 1р.

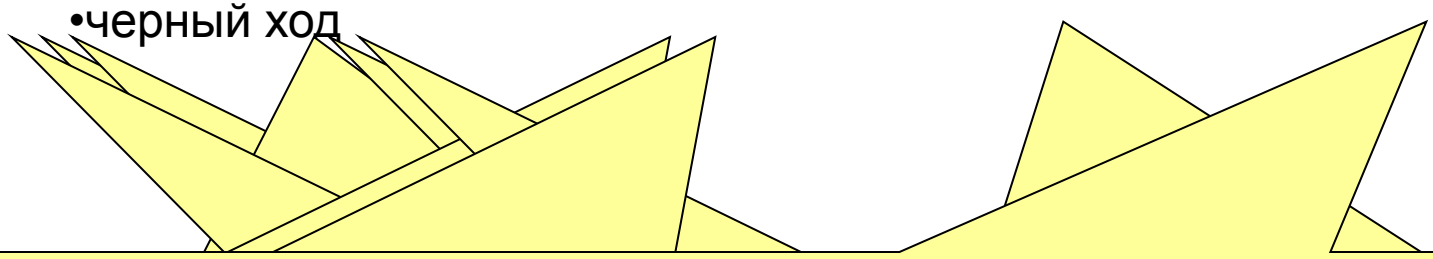
Внешний винчестер 250 Гб – 1300р. Цена за 1Гб – 5,2р.

Внешний винчестер 1 Тб – 2600р. Цена за 1Гб – 2,6р.

Промышленное ленточное резервирование

Потенциально-опасное программное обеспечение

- Потенциально вредоносное программное обеспечение
  - Вирус
  - Троянский
  - конь
  - Сетевой
  - червь
  - Закладка
  - Люк, брешь,
  - черный ход



Не описанная в документации возможность работы с данным программным продуктом.

Основные причины:

- забывчивость программиста;
- умышленно оставлено для облегчения отладки при внедрении и тестировании
- умышленно оставлено для скрытого управления уже работающим программным продуктом

chrome

Опасность: обнаружено вредоносное ПО!

Google Chrome заблокировал доступ к этой странице на сайте ria.ru.

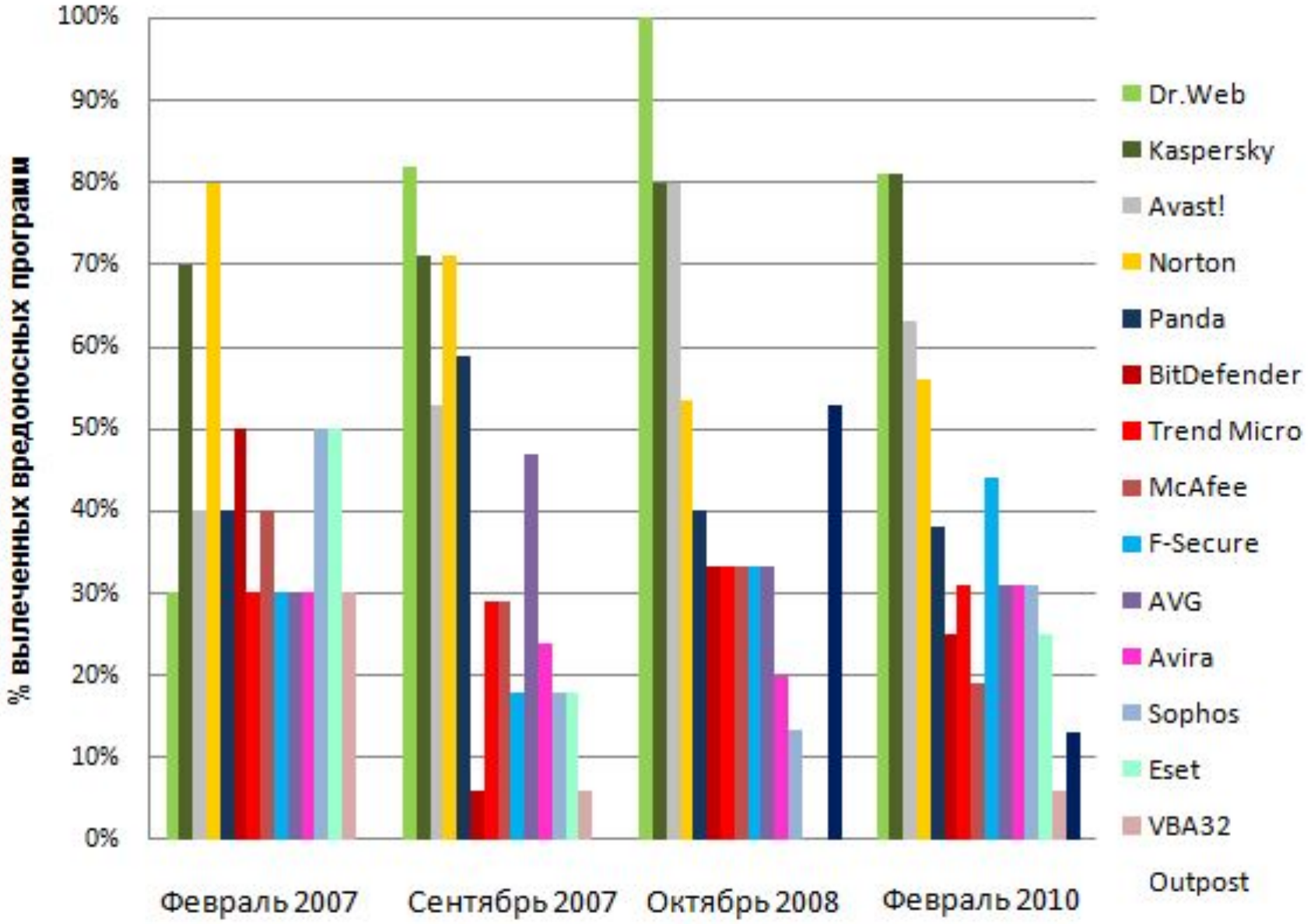
Эта страница содержит контент с сайта vid-1.rian.ru, который был замечен в распространении вредоносного ПО. Ее посещение может привести к заражению вашего компьютера.

Вредоносное ПО – это программное обеспечение, специально созданное для совершения преступных действий, например хищения идентификационных данных, кражи денег или безвозвратного удаления файлов.

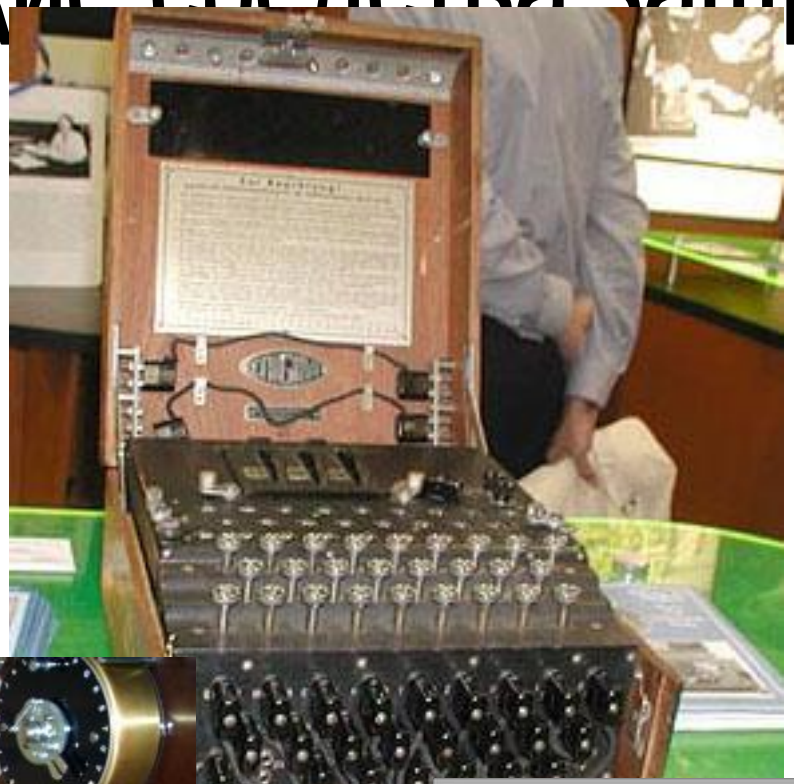
Подробнее...

Назад Дополнительно

☐ Помогать Google в улучшении системы обнаружения вредоносного ПО (при появлении подобных предупреждений в Google будут отправляться дополнительные сведения). "Политика конфиденциальности"


% вылеченных вредоносных программ
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
Февраль 2007
Сентябрь 2007
Октябрь 2008
Февраль 2010
Dr.Web
Kaspersky
Avast!
Norton
Panda
BitDefender
Trend Micro
McAfee
F-Secure
AVG
Avira
Sophos
Eset
VBA32
Outpost

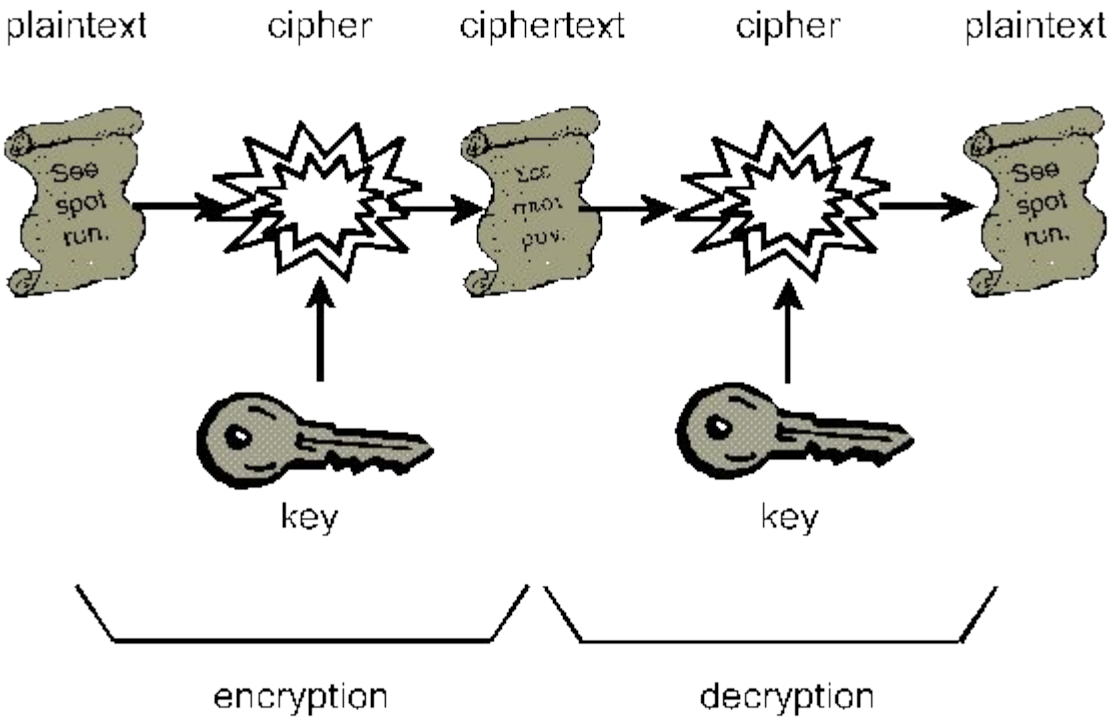
Криптографические средства защиты



Криптографические средства защиты

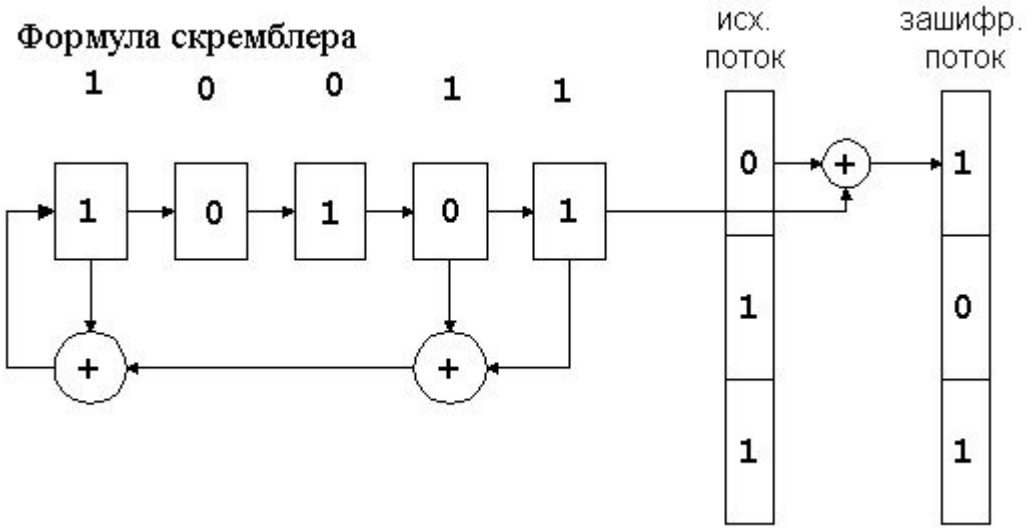
- Криптография
  - Тайнопись
  - Криптография
  - с ключом
    - Асимметричные
    - Симметричные
      - Поточные
      - Блочные

Симметричные криптоалгоритмы

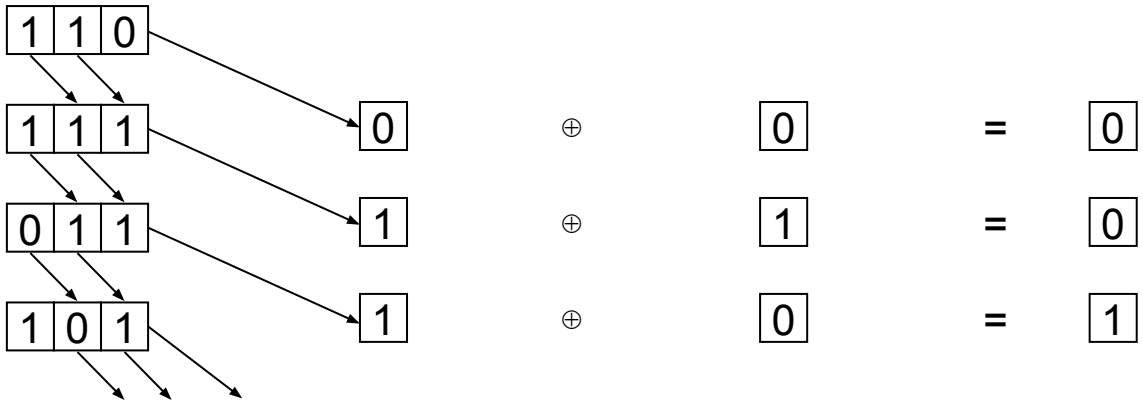


Криптографические средства защиты

Скремблеры (Scramble) – поточные шифры.



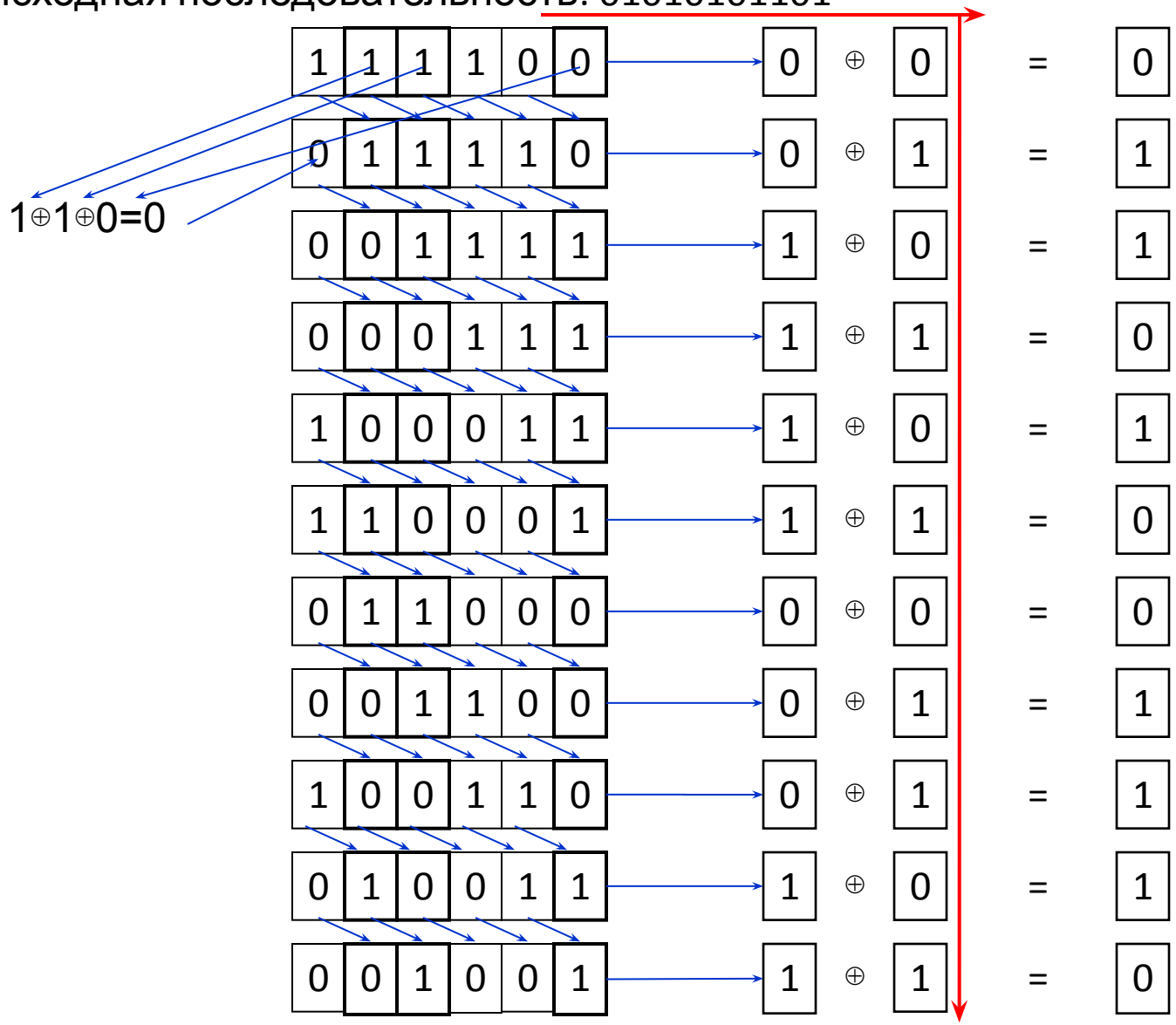
скремблер	кодирующий бит	информационный бит	результат



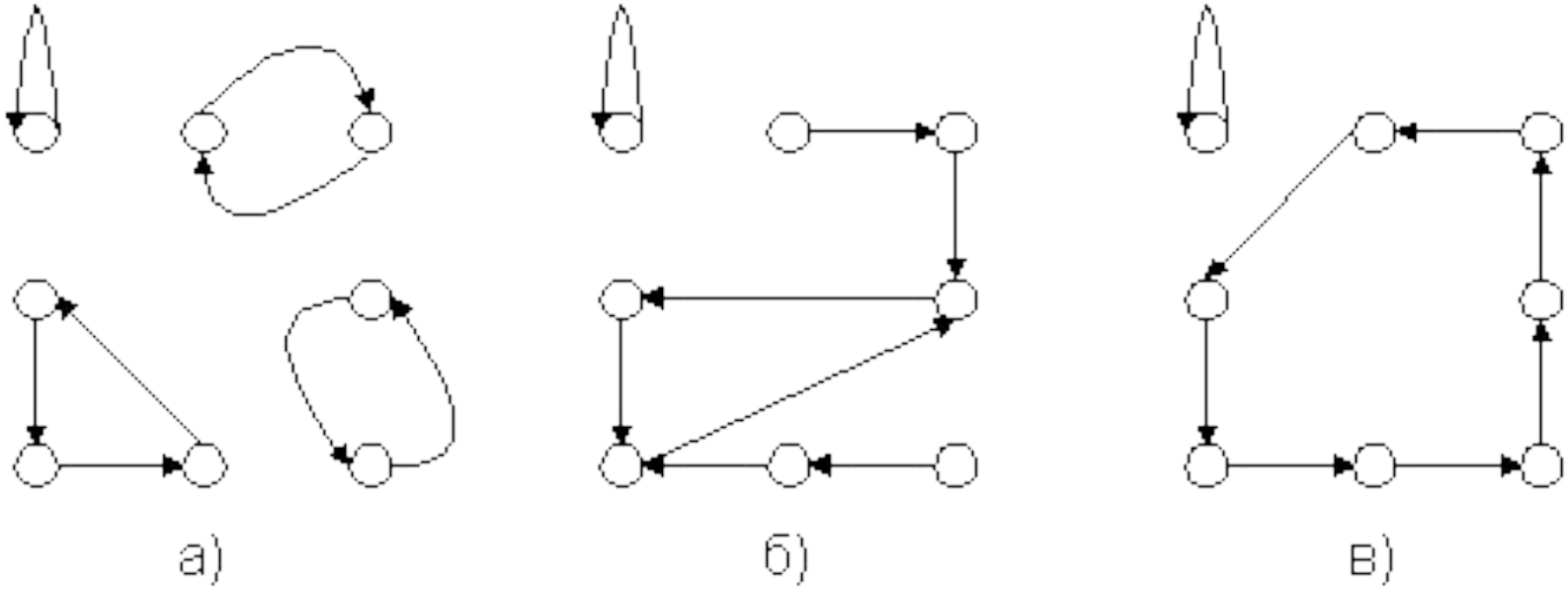
Формула скремблера: 011001

Начальный ключ: 111100

Исходная последовательность: 01010101101



Криптографические средства защиты



Графы состояний
скремблера

Криптографические средства защиты

Стойкие блочные криптоалгоритмы

Название алгоритма	**Автор**	**Размер блока**	**Длина ключа**
IDEA	Xuejia Lai James Massey	64 бита	128 бит
CAST128		64 бита	128 бит
BlowFish	Bruce Schneier	64 бита	128 – 448 бит
ГОСТ 28147-89	«Секретный» НИИ	64 бита	256 бит
TwoFish	Bruce Schneier	128 бит	128 – 256 бит
MARS	Корпорация IBM	128 бит	128 – 1048 бит

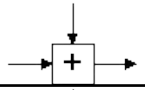
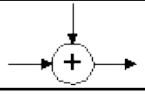
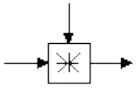
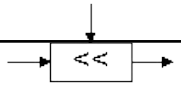
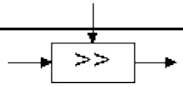
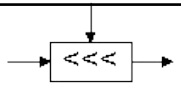
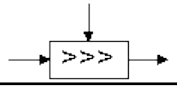
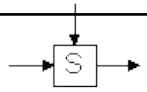
Криптографические средства защиты

На функцию стойкого блочного шифра Z = EnCrypt(X,Key) накладываются следующие условия:

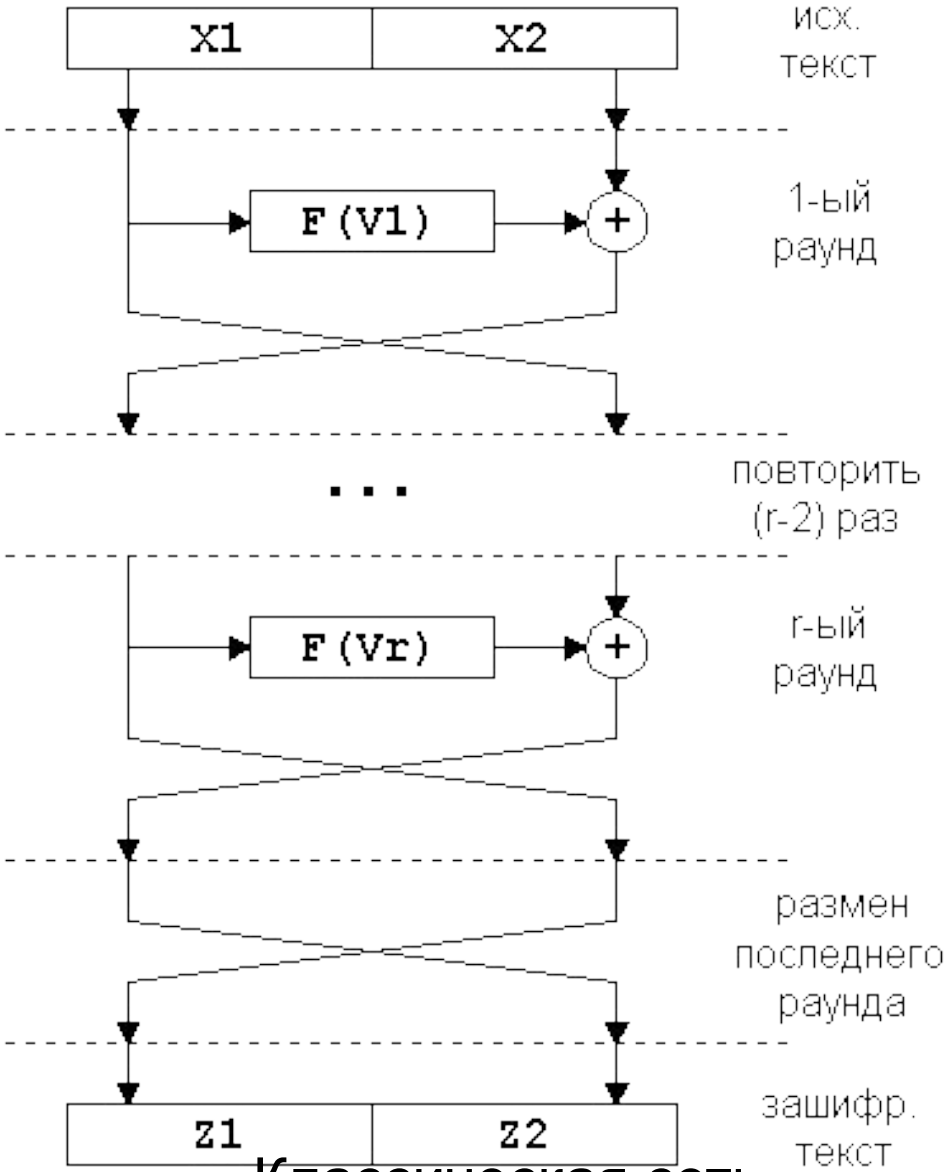
1. Функция EnCrypt должна быть обратимой.
2. Не должно существовать иных методов прочтения сообщения X по известному блоку Z, кроме как полным перебором ключей Key.
3. Не должно существовать иных методов определения, каким ключом Key было произведено преобразование известного сообщения X в сообщение Z, кроме как полным перебором ключей.

Криптографические средства защиты

Функции, используемые в криптоалгоритмах

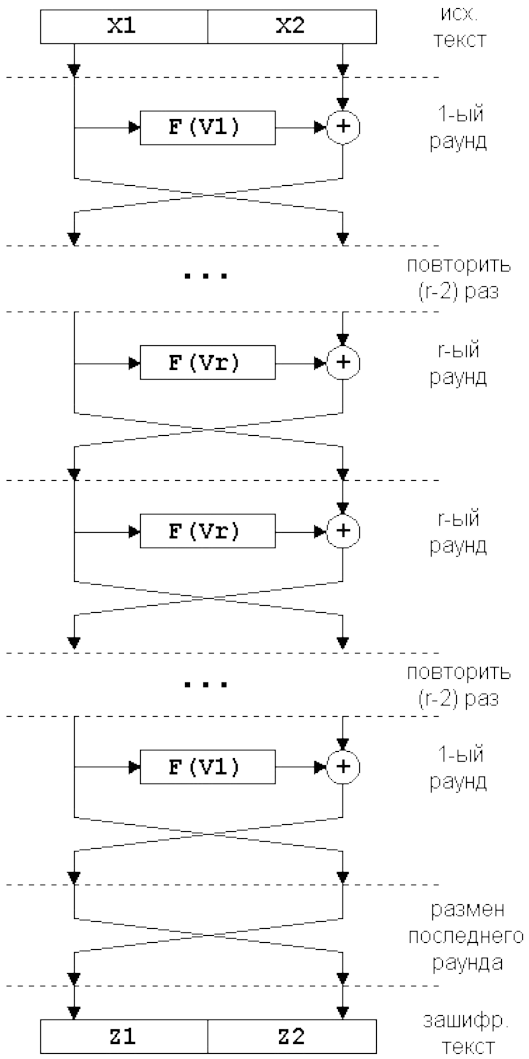
Биективные математические функции		
	Сложение	X' = X + V
	Исключающее ИЛИ	X' = X XOR V
	Умножение по модулю 2^N+1	X' = (X*V) mod (2^N + 1)
	Умножение по модулю 2^N	X' = (X*V) mod (2^N)
Битовые сдвиги		
	Арифметический сдвиг влево	X' = X SHL V
	Арифметический сдвиг вправо	X' = X SHR V
	Циклический сдвиг влево	X' = X ROL V
	Циклический сдвиг вправо	X' = X ROR V
Табличные подстановки		
	S-box (англ. substitute)	X' = Table[X, V]

Криптографические средства защиты



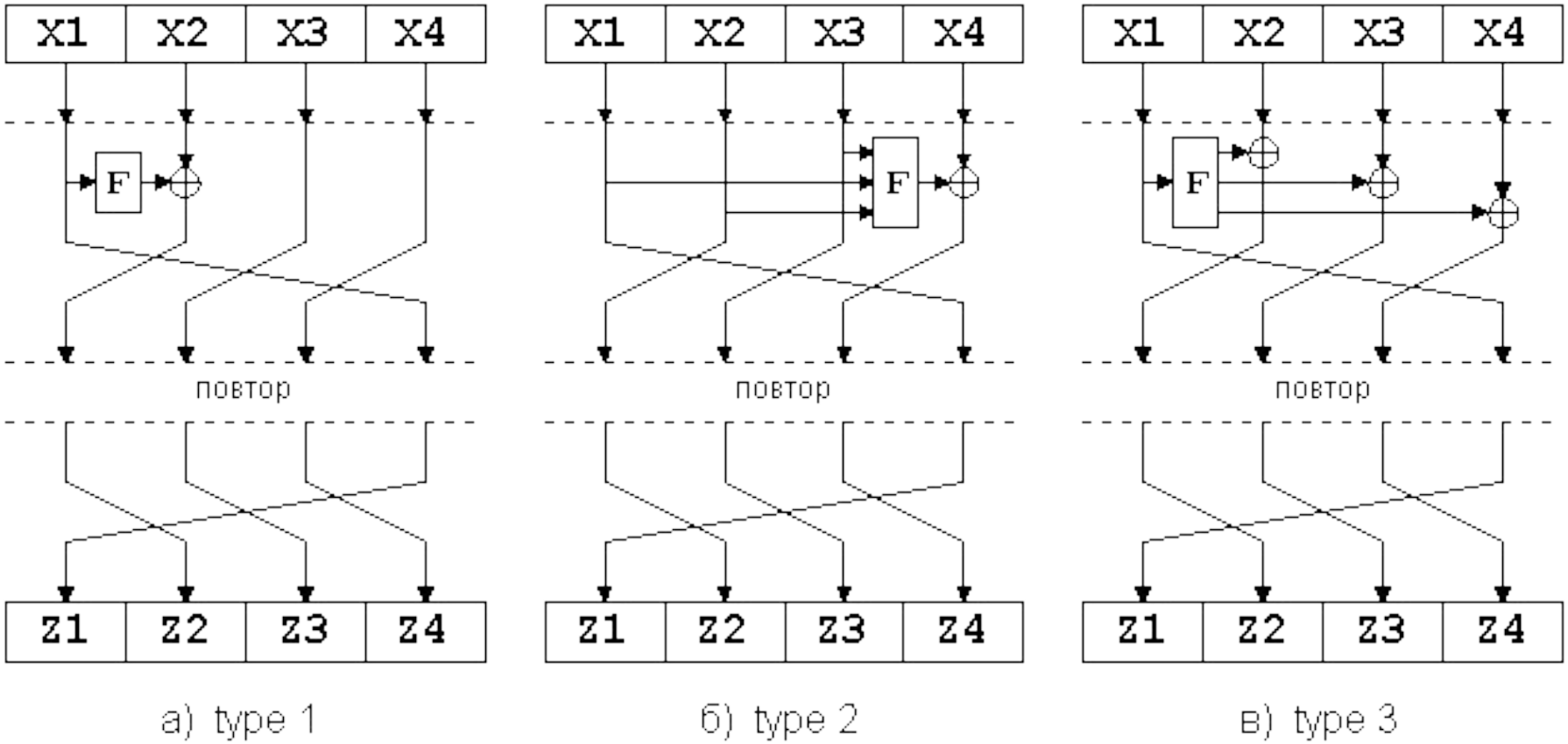
Классическая сеть Фейштеля

Криптографические средства защиты



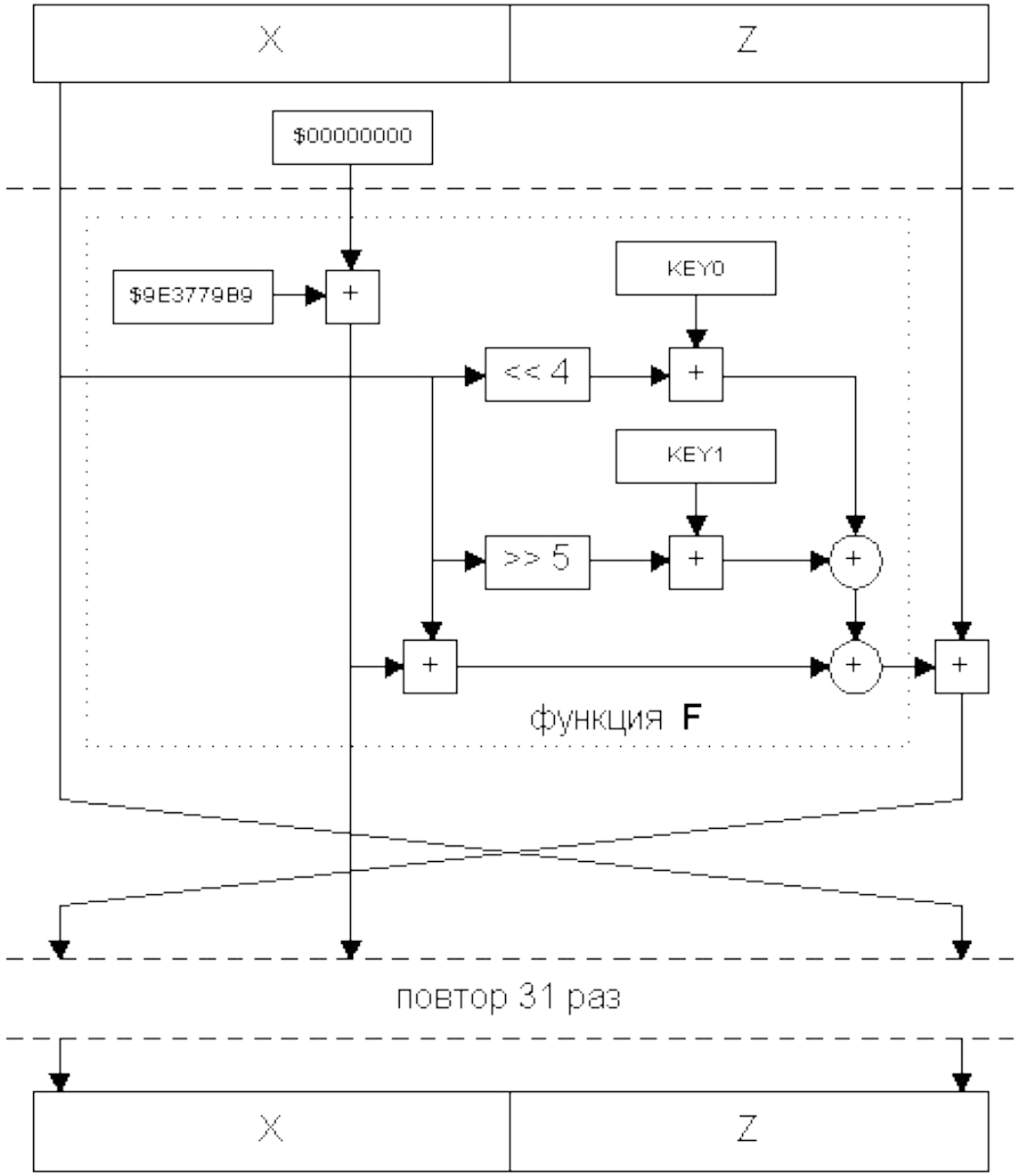
Симметричная сеть Фейштеля

Криптографические средства защиты



Модификации сети Фейштеля

Криптографические средства защиты



Алгоритм TEA – Tiny Encryption Algorithm

Криптографические средства защиты

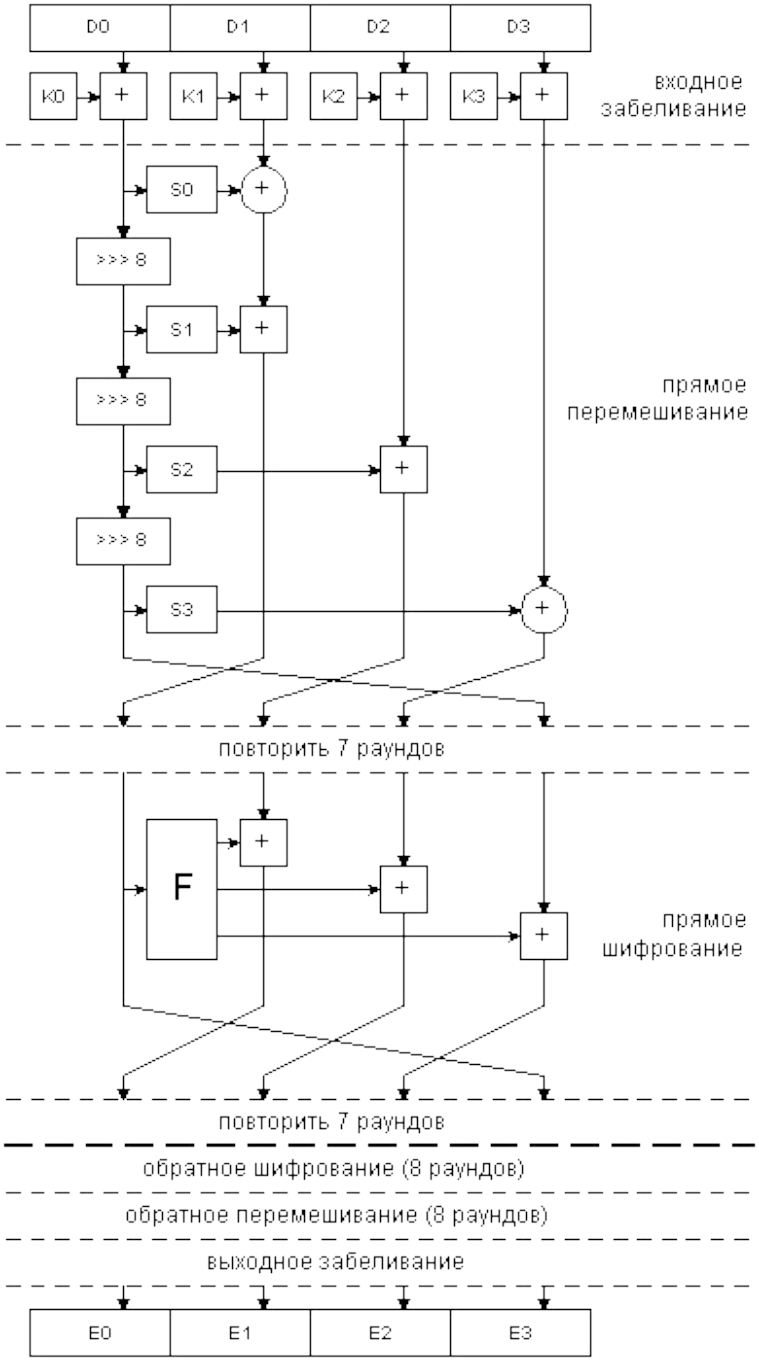
Требования к шифрам на конкурсе AES:

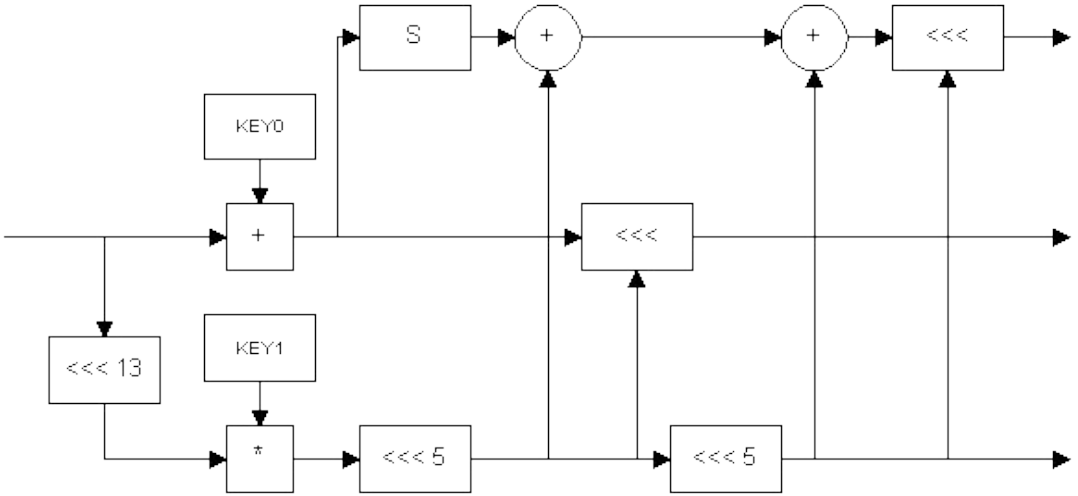
– алгоритм должен быть симметричным;
– алгоритм должен быть блочным шифром;
– алгоритм должен иметь длину блока 128 бит и поддерживать три длины ключа : 128, 192 и 256 бит;

Финалисты конкурса AES

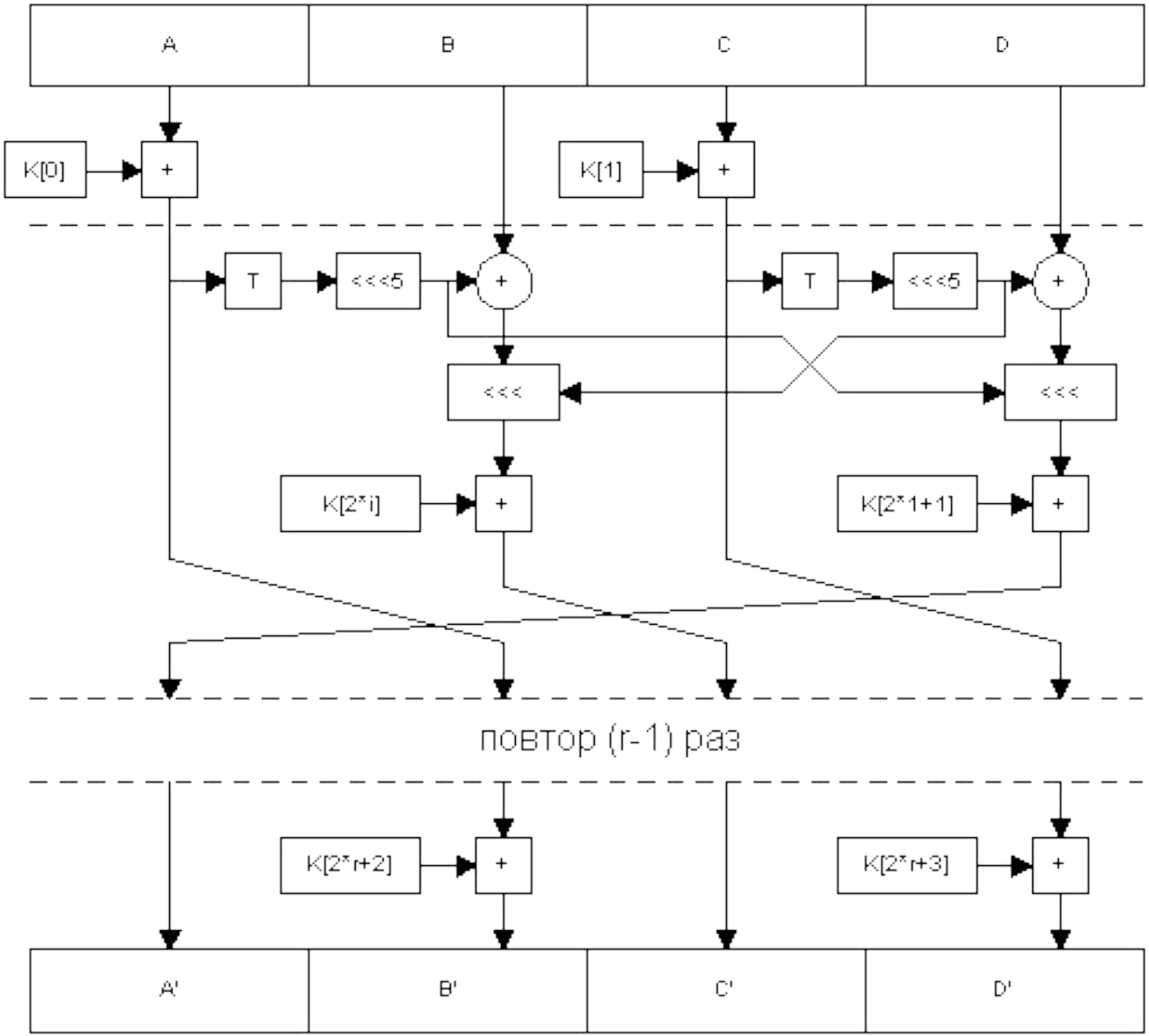
Алгоритм	**Создатель**	**Страна**	**Быстродействие (asm, 200МГц)**
MARS	IBM	США	8 Мбайт/с
RC6	R.Rivest & Co	США	12 Мбайт/с
Rijndael	V.Rijmen & J.Daemen	Бельгия	7 Мбайт/с
Serpent	*Университеты*	Израиль, Великобритания, Норвегия	2 Мбайт/с
TwoFish	B.Schneier & Co	США	11 Мбайт/с

Криптоалгоритм MARS

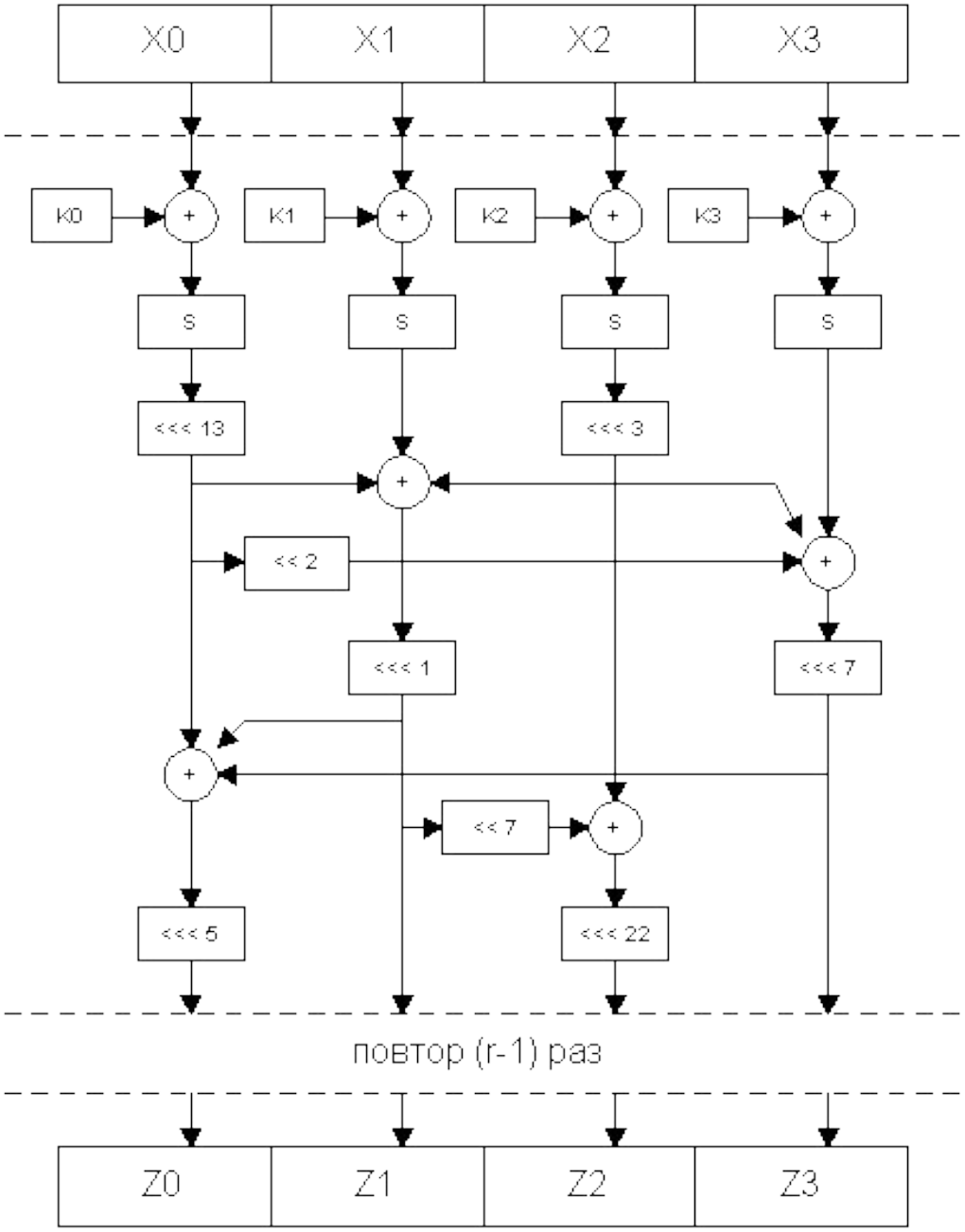




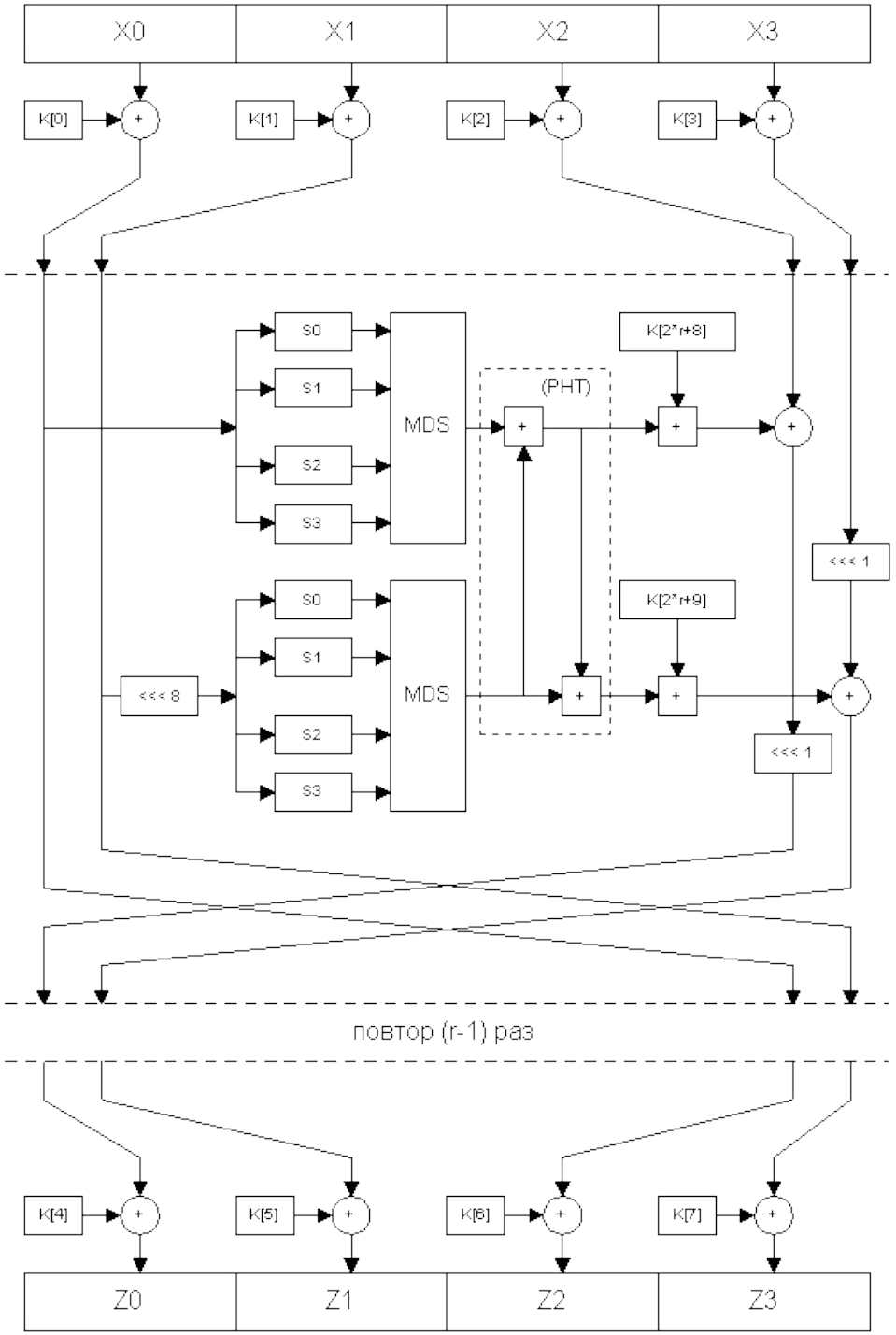
Криптоалгоритм RC6



Криптоалгоритм Serpent

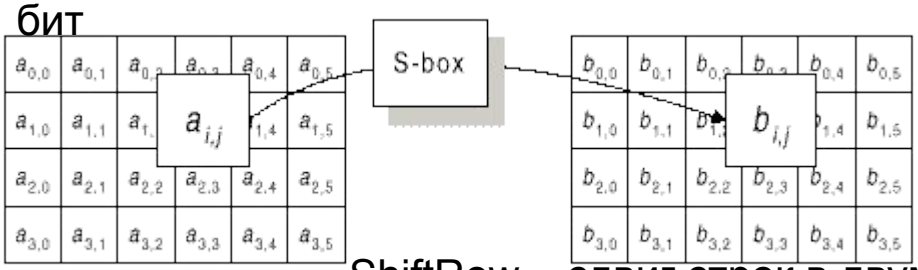


Криптоалгоритм TwoFish

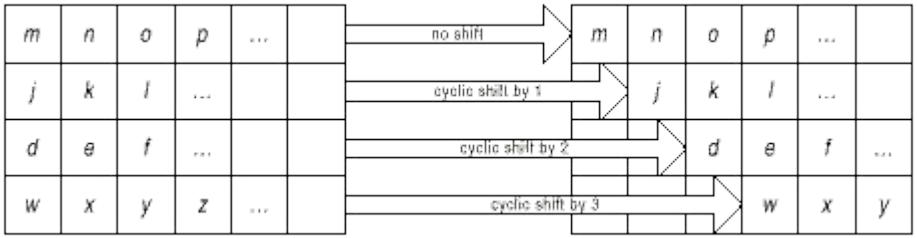


Криптоалгоритм Rijndael

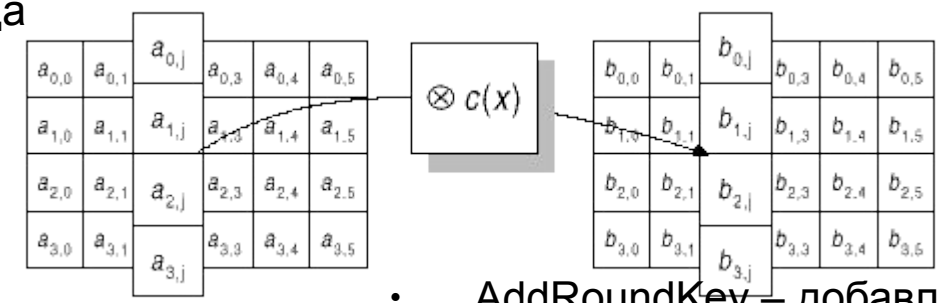
- ByteSub – табличная подстановка 8x8 бит



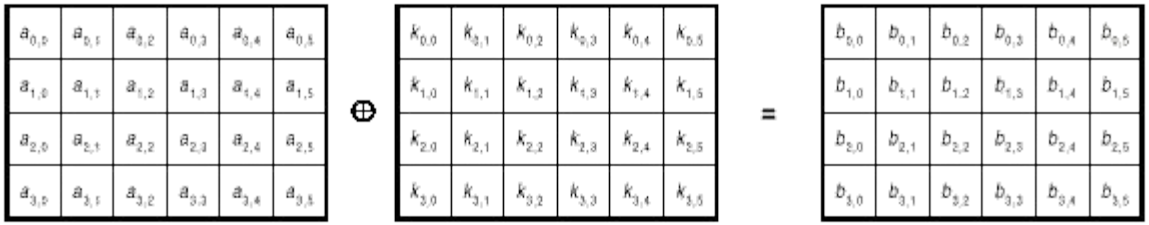
ShiftRow – сдвиг строк в двумерном массиве на различные смещения



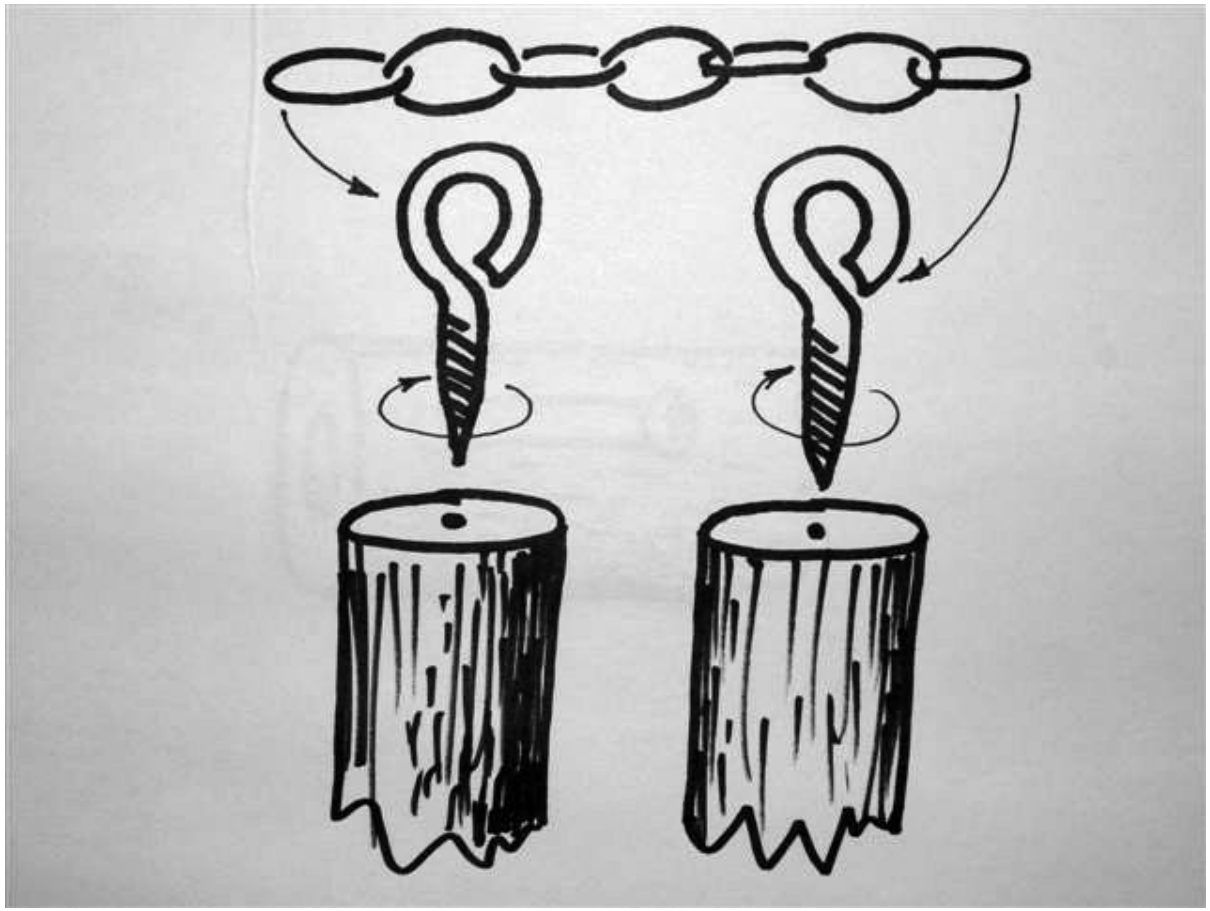
MixColumn – математическое преобразование, перемешивающее данные внутри лбца



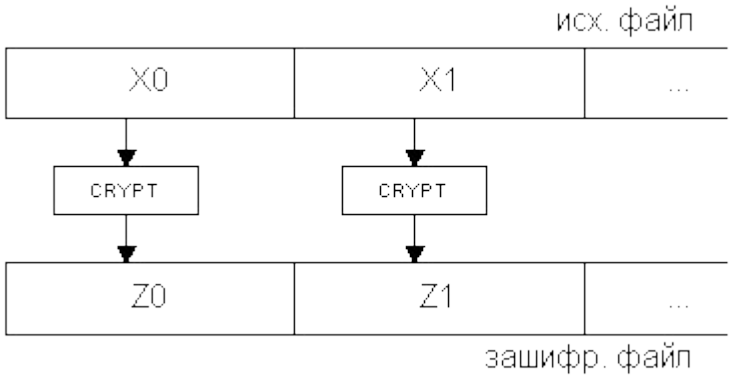
- AddRoundKey – добавление материала ключа операцией XOR



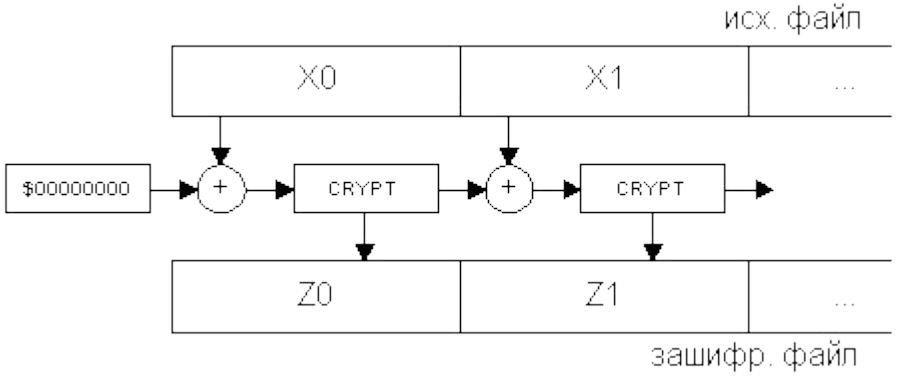
Алгоритмы создания криптоцепочек



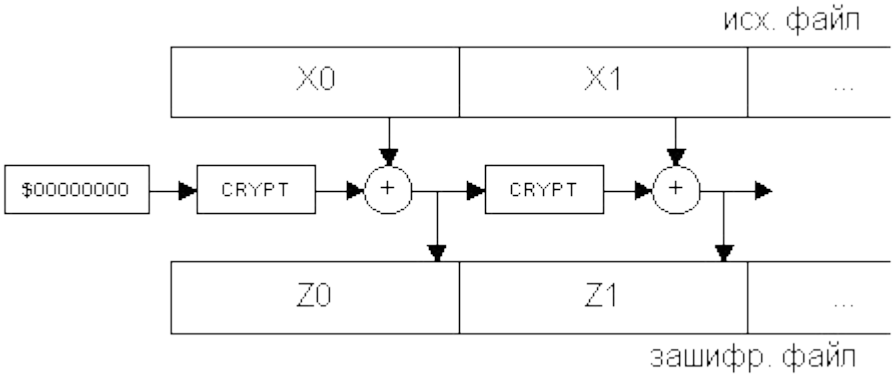
Алгоритмы создания криптоцепочек



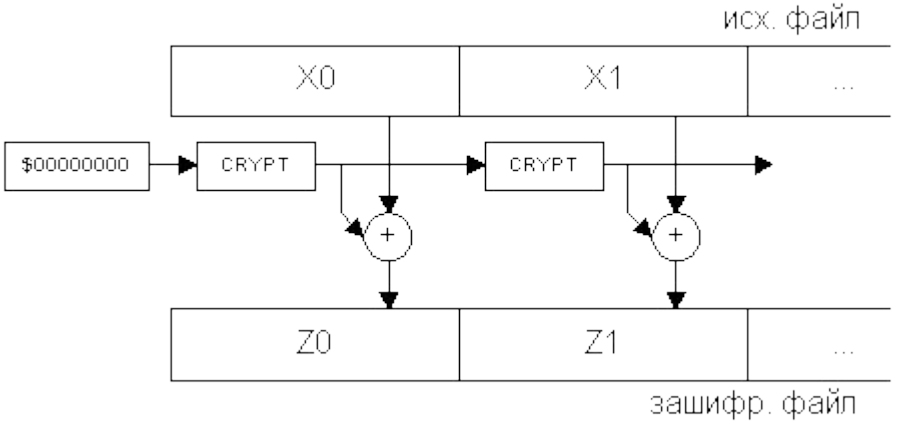
ECB – Electronic CodeBook



CBC – Cipher Block Chaining



CFB – Cipher FeedBack

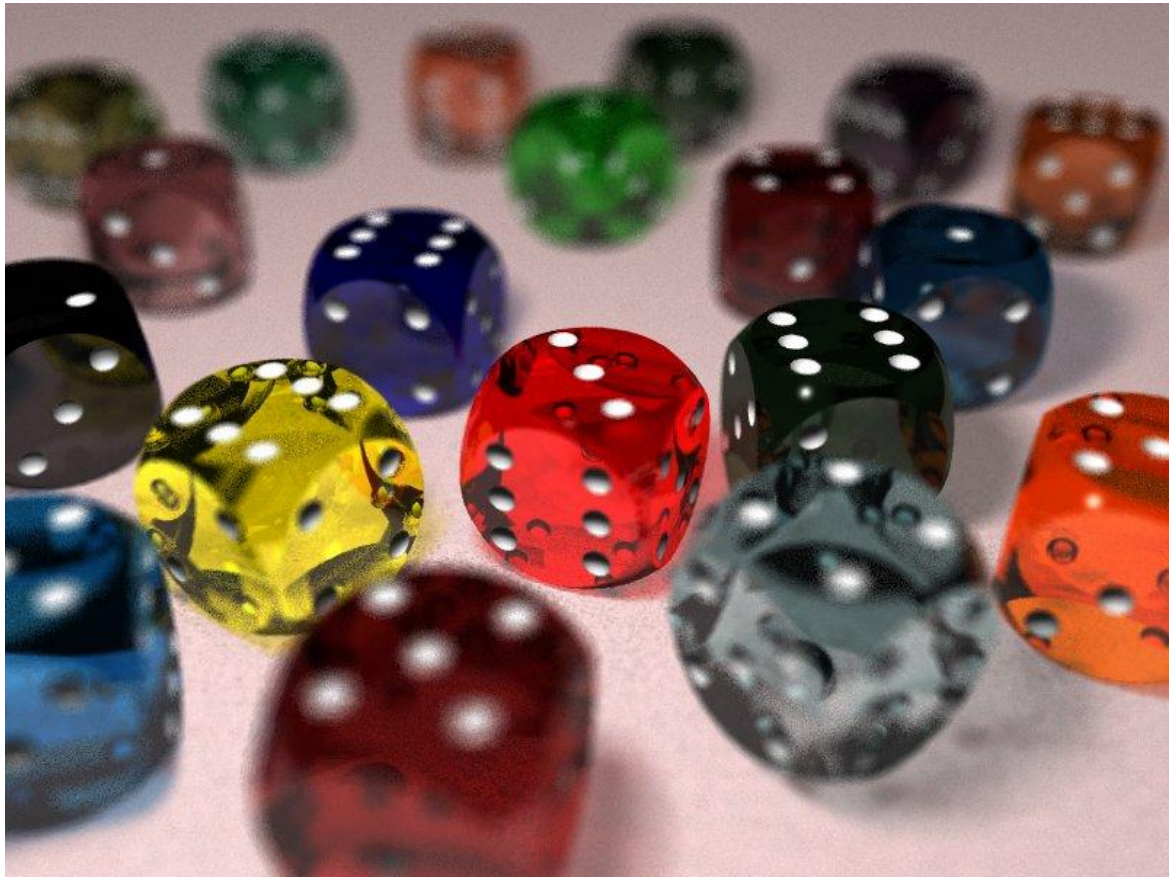


OFB – Output FeedBack

Алгоритмы создания криптоцепочек

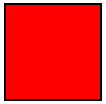
Метод	Шифрование блока зависит от	Искажение одного бита при передаче	Кодируется ли некратное блоку число байт без дополнения?	На выход криптосистемы поступает
ECB	текущего блока	портит весь текущий блок	нет	выход криптоалгоритма
CBC	всех предыдущих блоков	портит весь текущий и все последующие блоки	нет	выход криптоалгоритма
CFB	всех предыдущих блоков	портит один бит текущего блока и все последующие блоки	да	XOR маска с исходным текстом
OFB	позиции блока в файле	портит только один бит текущего блока	да	XOR маска с исходным текстом

Рандомизация сообщений



Рандомизация сообщений

Исходный файл



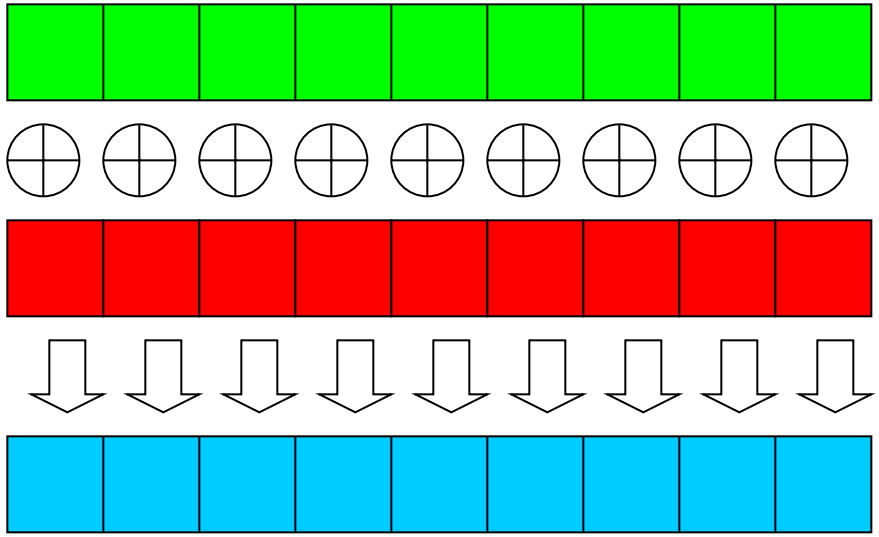
Псевдослучайная последовательность

Результирующий файл на отправку

Запись в начало файла данных псевдослучайной последовательности байт заранее оговоренной длины с отбрасыванием ее при дешифровании – этот метод будет работать только при применении алгоритмов создания цепочек с памятью (CBC,CFB,OFB),

Рандомизация сообщений

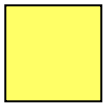
Фиксированная случайная величина



Смешивание каждого блока исходного файла со случайной величиной

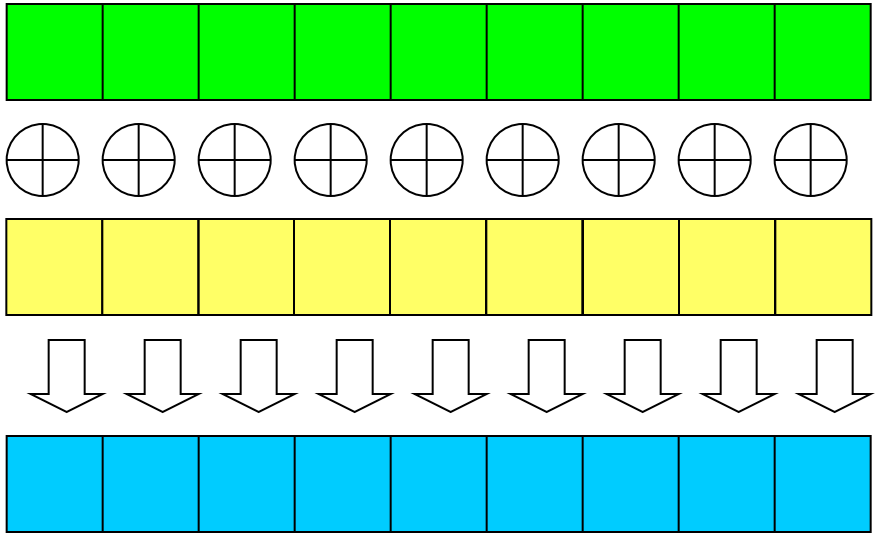
Результирующий файл на отправку

Рандомизация сообщений



Заранее оговоренная величина

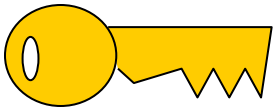
Величина, зашифрованная тем же ключом и шифром



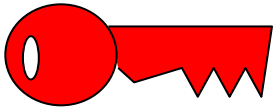
Смешивание каждого блока исходного файла с вычисленным значением

Результирующий файл на отправку

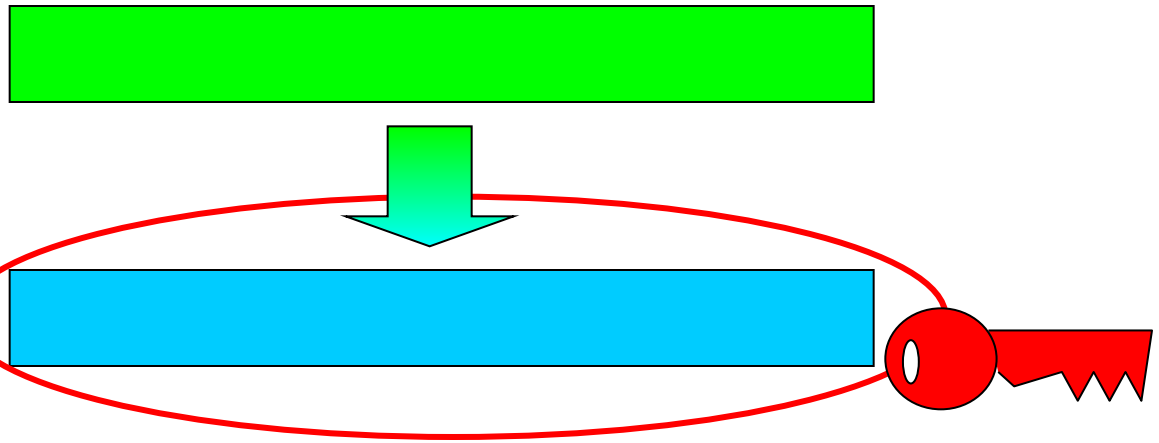
Рандомизация сообщений



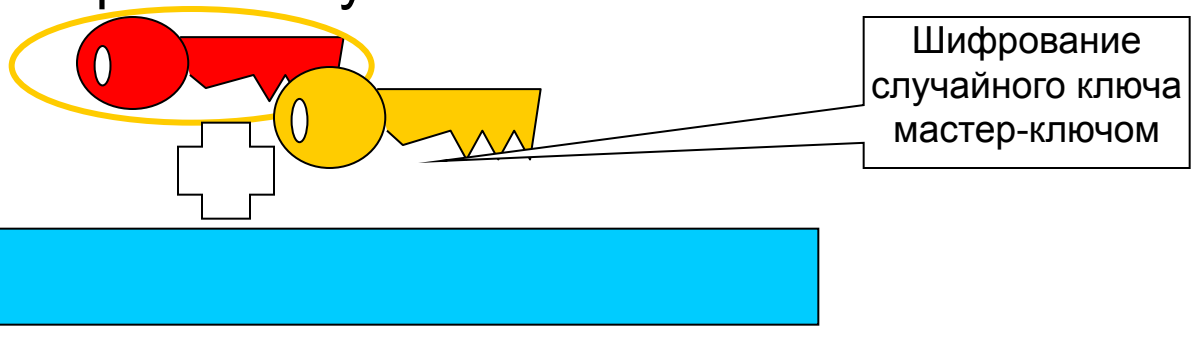
Первоначальный мастер-ключ



Случайный ключ для данного файла



Шифрование файла случайным ключом

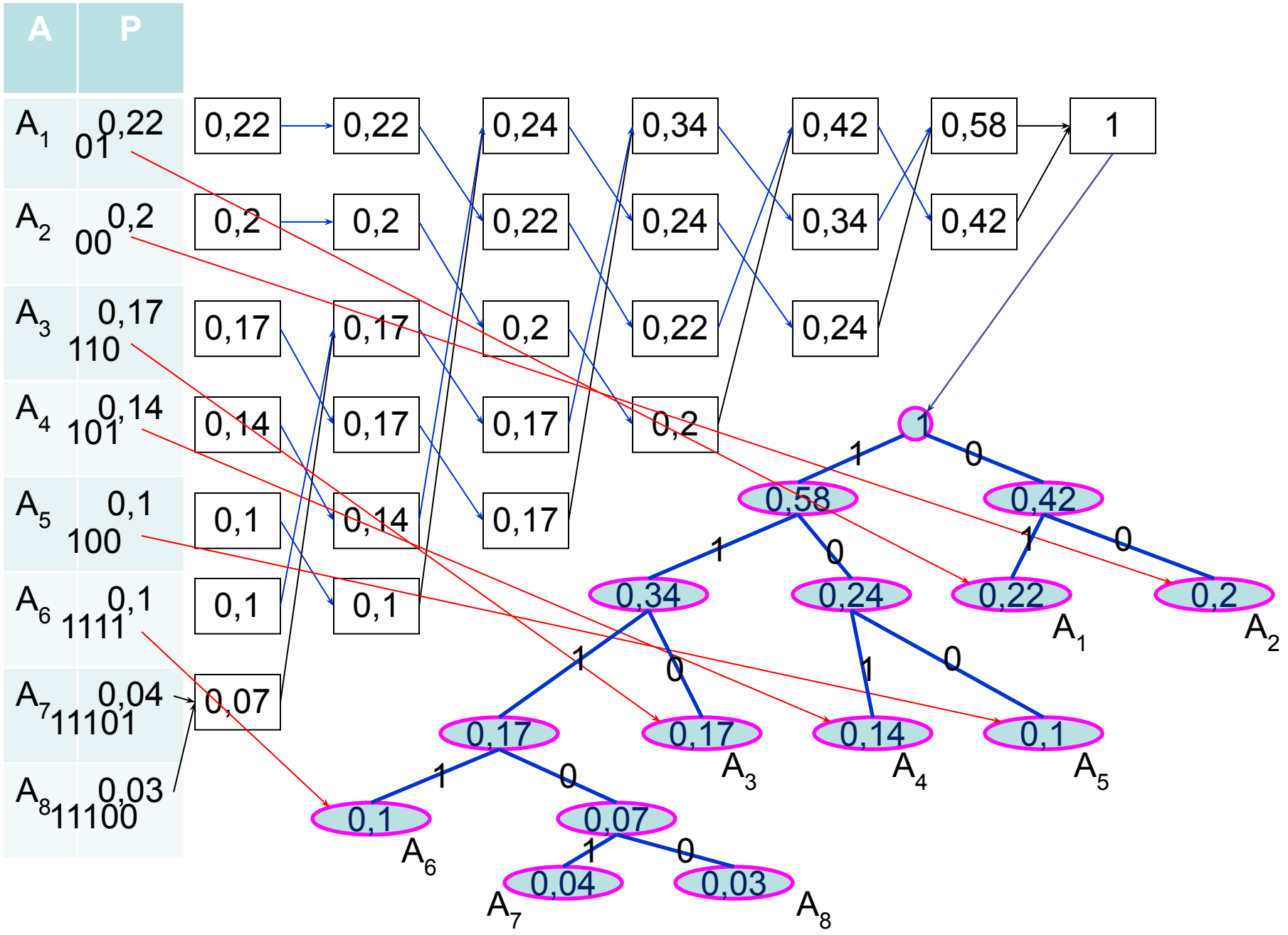


Результирующий файл на отправку

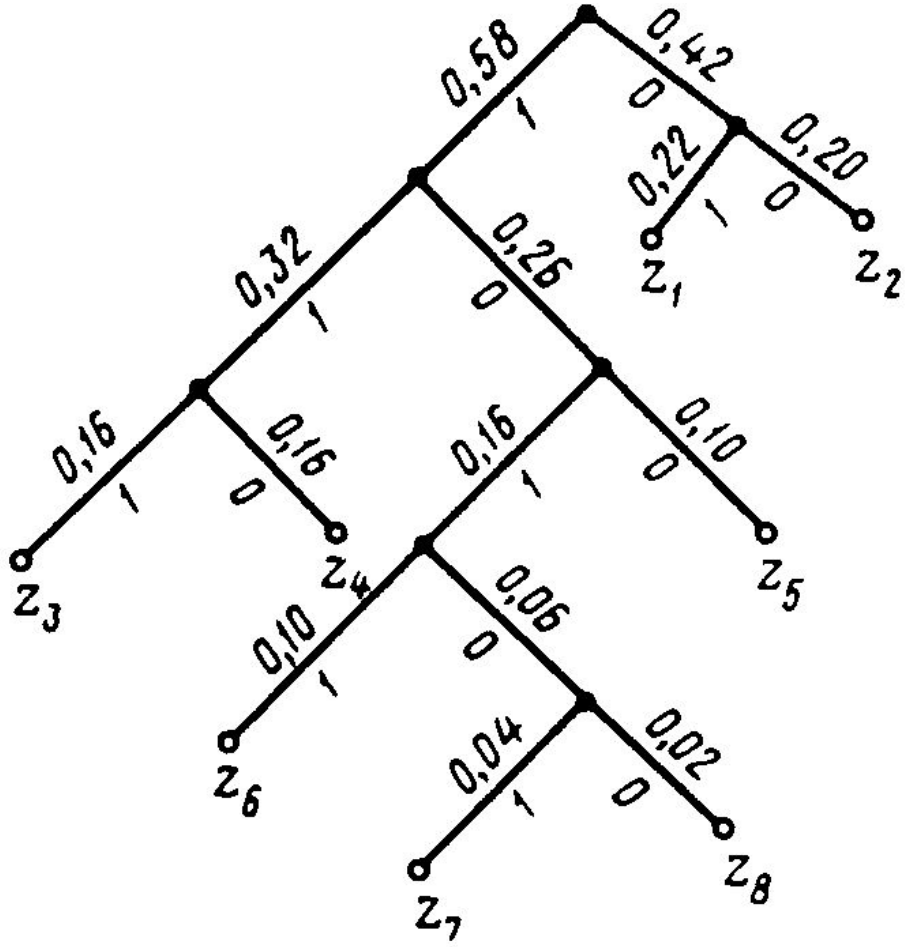
Алгоритмы сжатия информации

Буквы	Вероятности
z_1	0,22
z_2	0,20
z_3	0,16
z_4	0,16
z_5	0,10
z_6	0,10
z_7	0,04
z_8	0,02

Алгоритм Хаффмана (Huffman)


A
P
A1 0,22 01
A2 0,2 00
A3 0,17 110
A4 0,14 101
A5 0,1 100
A6 0,1 1111
A7 0,04 11101
A8 0,03 11100
0,22
0,2
0,17
0,14
0,1
0,07
0,22
0,2
0,17
0,17
0,14
0,1
0,24
0,22
0,2
0,17
0,17
0,34
0,24
0,22
0,2
0,42
0,34
0,24
0,58
0,42
1
1
0,58
0,42
0,34
0,24
0,22
0,2
A1
A2
0,17
0,17
0,14
0,1
A3
A4
A5
0,1
0,07
0,04
0,03
A6
A7
A8

Буквы	Вероятности	Вспомогательные столбцы						
		1	2	3	4	5	6	7
Z_1	0,22	0,22	0,22	0,26	0,32	0,42	0,58	1
Z_2	0,20	0,20	0,20	0,22	0,26	0,32	0,42	
Z_3	0,16	0,16	0,16	0,20	0,22	0,26		
Z_4	0,16	0,16	0,16	0,16	0,20			
Z_5	0,10	0,10	0,16	0,16				
Z_6	0,10	0,10	0,10					
Z_7	0,04	0,06						
Z_8	0,02							



z_1	z_2	z_3	z_4	z_5	z_6	z_7	z_8
01	00	111	110	100	1011	10101	10100

Алгоритм Лемпела-Зива (Lempel-Ziv)

Классический алгоритм Лемпеля-Зива – LZ77, названный так по году своего опубликования, предельно прост. Он формулируется следующим образом : **"если в прошедшем ранее выходном потоке уже встречалась подобная последовательность байт, причем запись о ее длине и смещении от текущей позиции короче чем сама эта последовательность, то в выходной файл записывается ссылка (смещение, длина), а не сама последовательность"**.

"КОЛОКОЛ_ОКОЛО_КОЛОКОЛЬНИ"

"КОЛО(-4,3)_(-5,4)О_(-14,7)ЬНИ"

Алгоритм RLE (англ. Run Length Encoding)

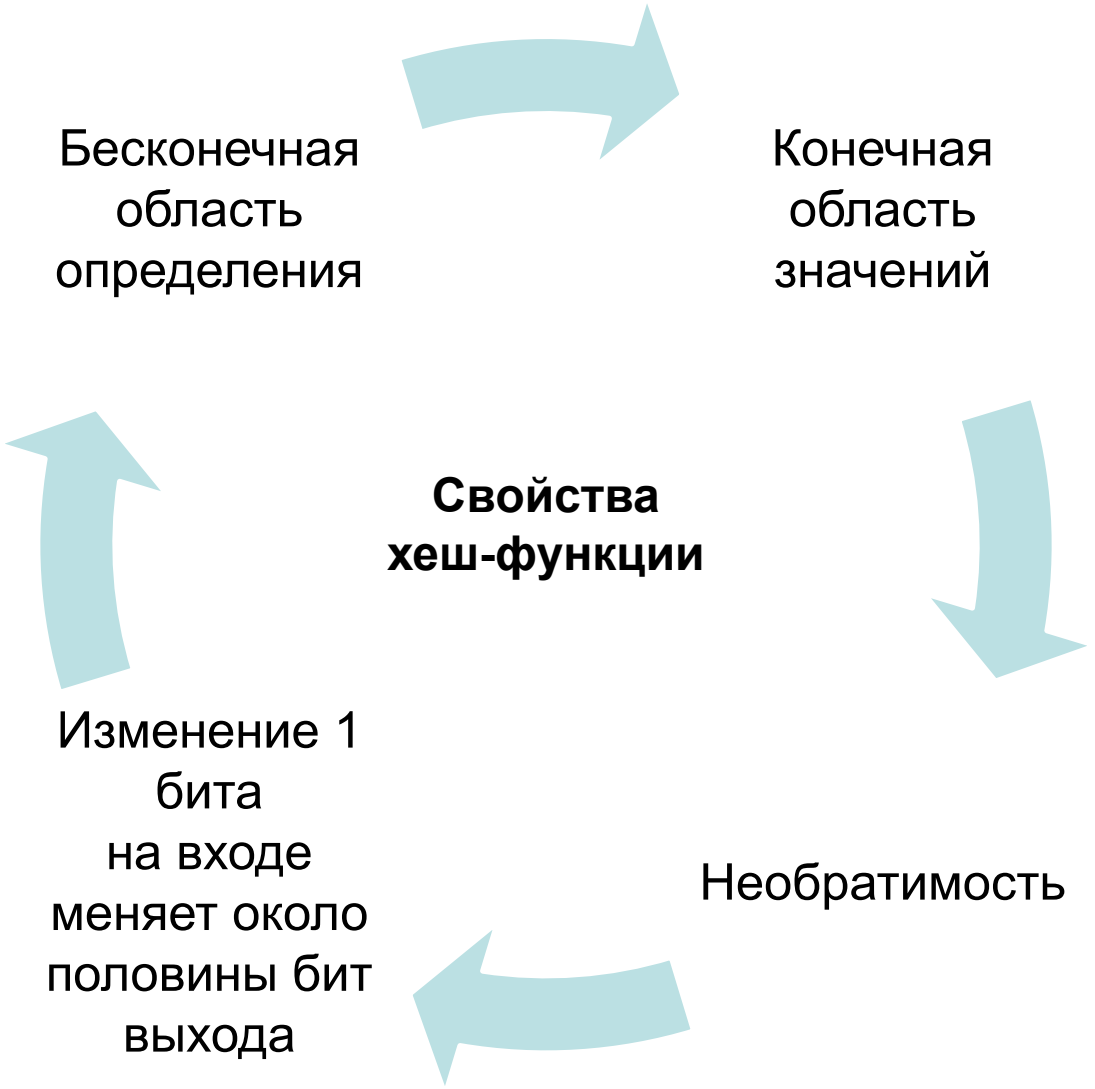
"AAAAAAA"

"(A,7)"

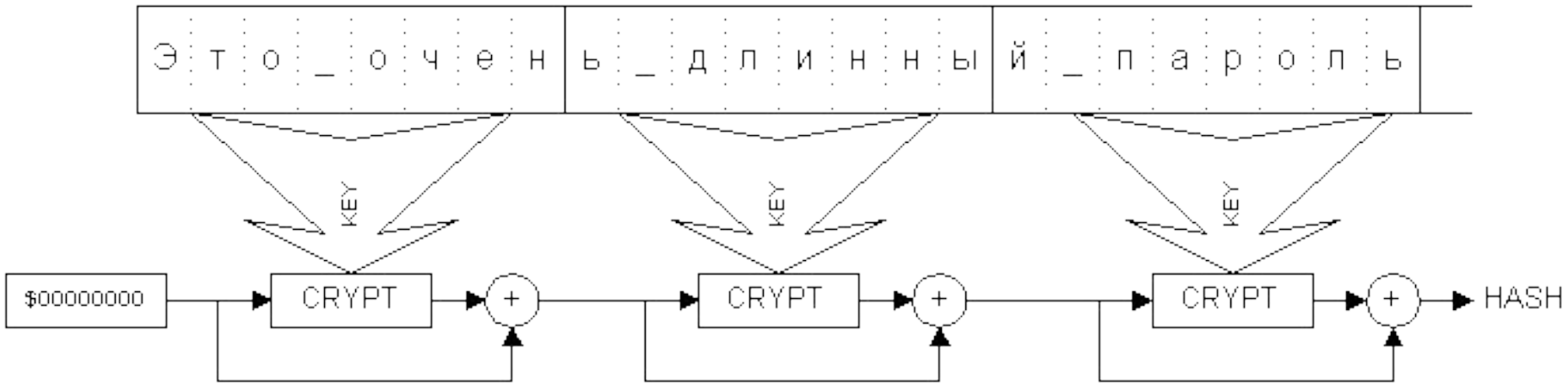
Хеширование

Хеширование

Хеширование, от англ. to hash – нарезать, измельчать



Хеширование



Классическая схема хеширования

Хеширование

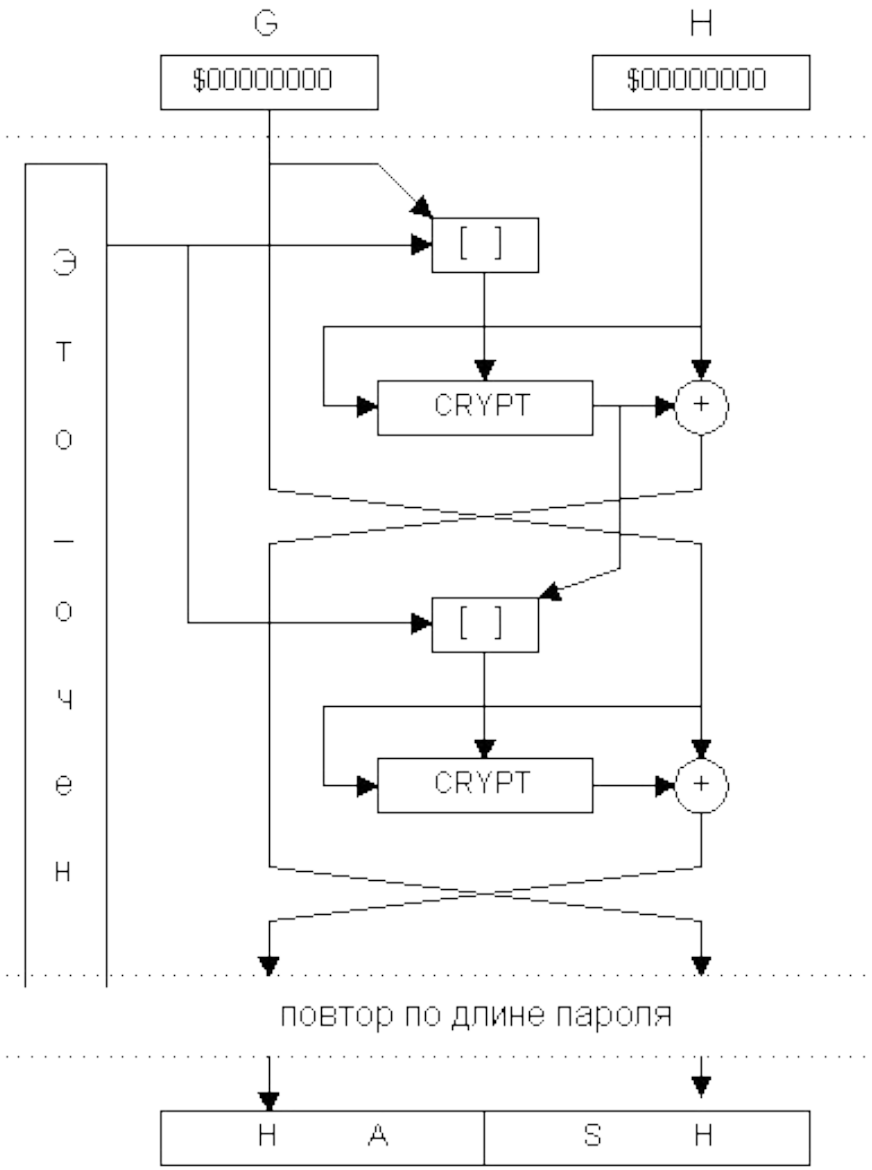
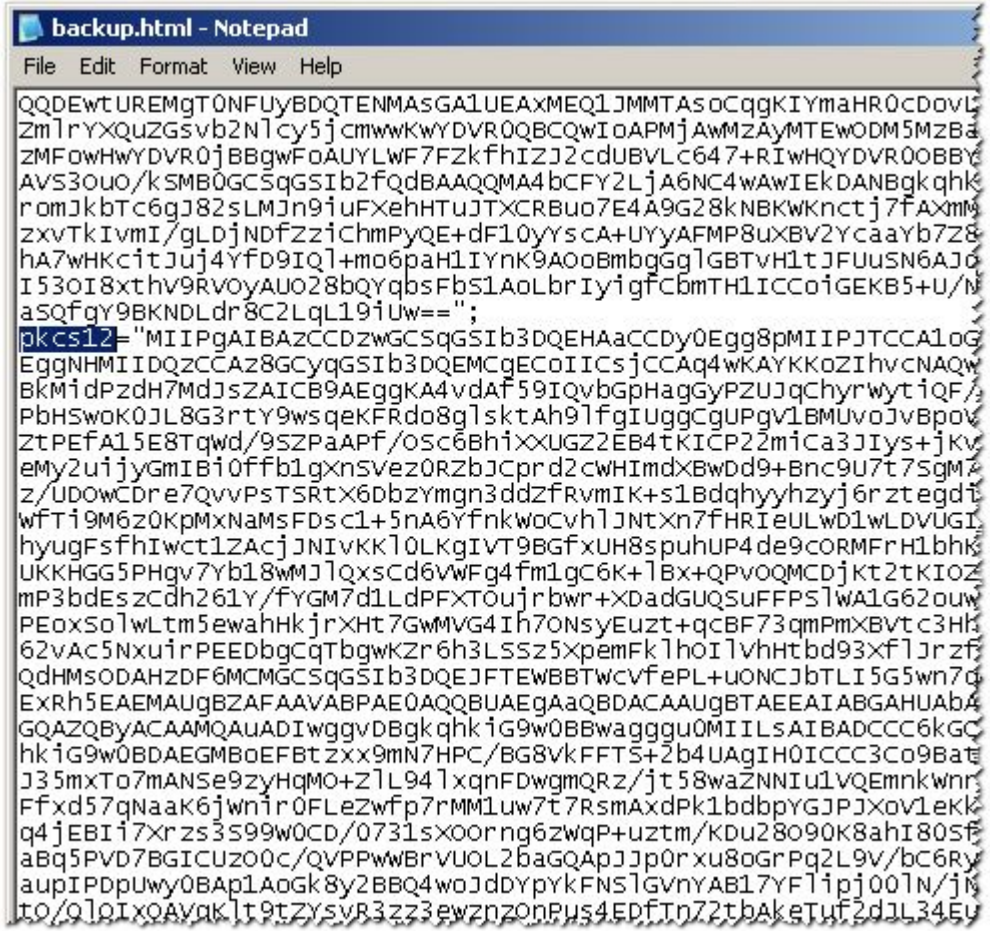


Схема хеширования по алгоритму Tandem DM

(авторы Девис и Майер)

Транспортное кодирование



Транспортное кодирование

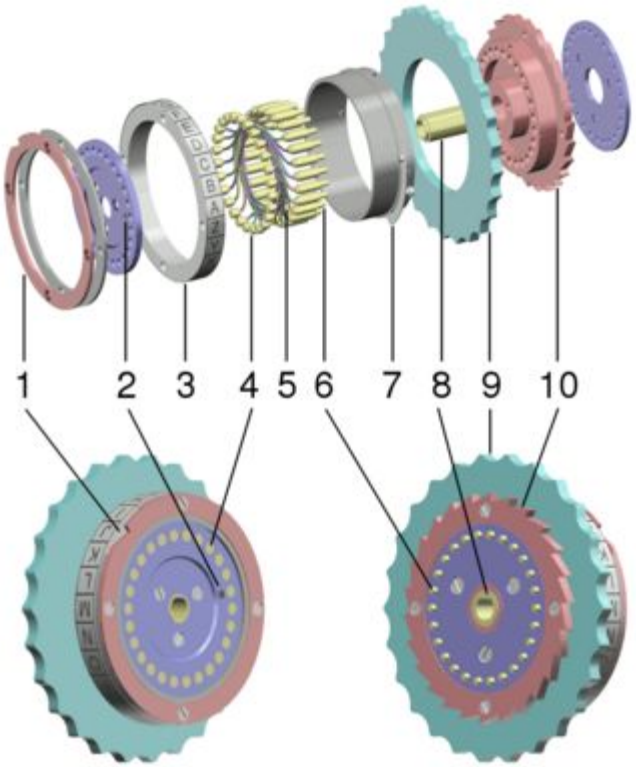
код	значение	код	значение	код	значение	код	значение
A	0	Q	16	g	32	w	48
B	1	R	17	h	33	x	49
C	2	S	18	i	34	y	50
D	3	T	19	j	35	z	51
E	4	U	20	k	36	1	52
F	5	V	21	l	37	2	53
G	6	W	22	m	38	3	54
H	7	X	23	n	39	4	55
I	8	Y	24	o	40	5	56
J	9	Z	25	p	41	6	57
K	10	a	26	q	42	7	58
L	11	b	27	r	43	8	59
M	12	c	28	s	44	9	60
N	13	d	29	t	45	0	61
O	14	e	30	u	46	+	62
P	15	f	31	v	47	/	63
Алфавит кодировки BASE64						заполнитель	=

Транспортное кодирование

Исходные символы	**C**	**a**	**t**
ASCII коды (десятич.)	**67**	**97**	**116**
ASCII (двоичн.)	0 1 0 0 0 0 1 1	0 1 1 0 0 0 0 1	0 1 1 1 0 1 0 0
Новые десятичные значения	**16**	**54**	**5**	**52**
+32	**48**	**86**	**37**	**84**
Символы UUE	**0**	**V**	**%**	**T**

Пример кодирования в кодировке UUE

Функции симметричных криптосистем



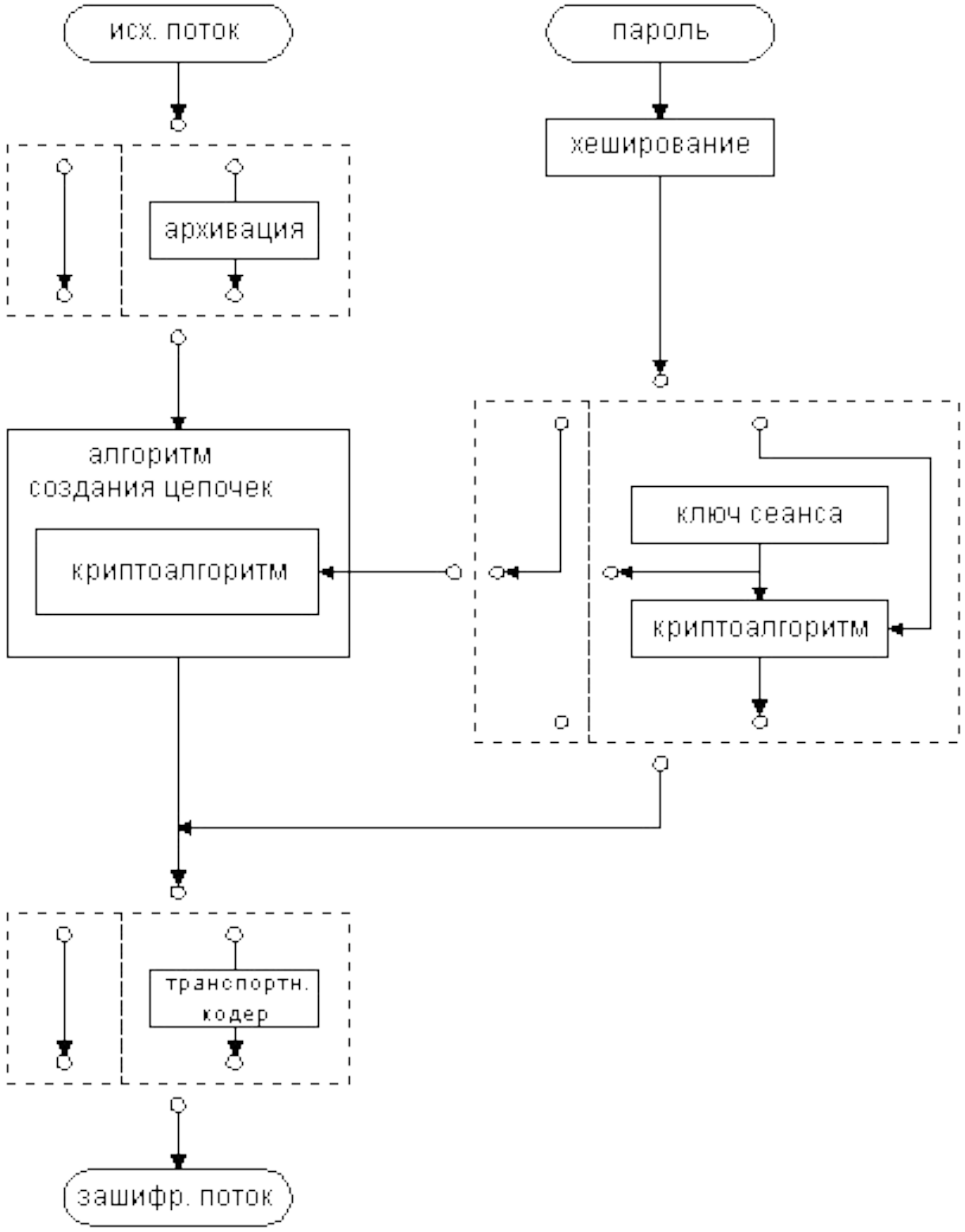
Криптосистема – это завершенная комплексная модель, способная производить двусторонние криптопреобразования над данными произвольного объема и подтверждать время отправки сообщения, обладающая механизмом преобразования паролей и ключей и системой транспортного кодирования.

Таким образом, криптосистема выполняет **три основные функции**:

- усиление защищенности данных,
- облегчение работы с криптоалгоритмом со стороны человека
- обеспечение совместимости потока данных с другим программным обеспечением.

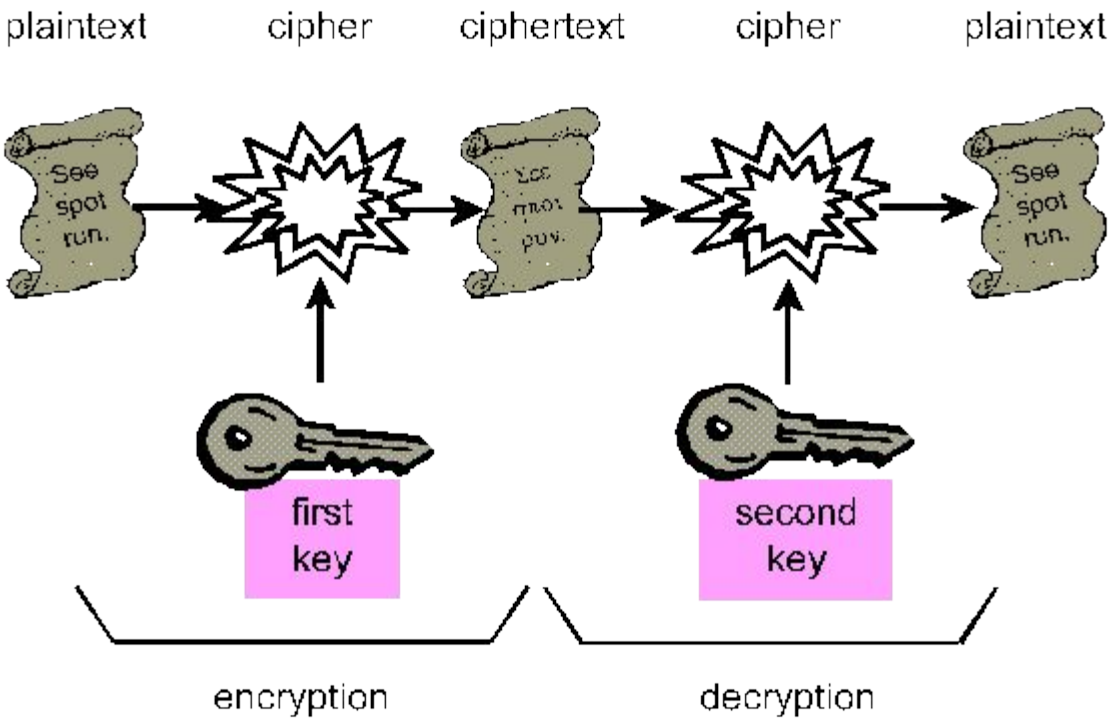
Конкретная программная реализация криптосистемы называется **криптопакетом.**

:) Первое краткое резюме :)



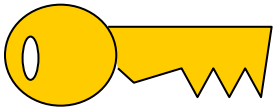
Общая схема симметричной криптосистемы

Асимметричные криптоалгоритмы



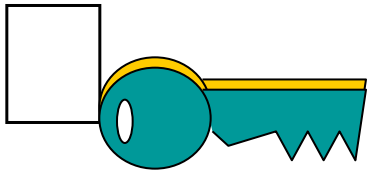
Открытый ключ Пети

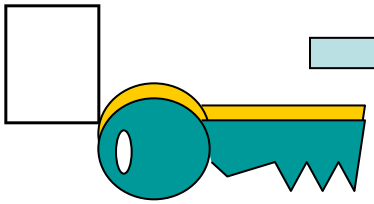
Ключ Васи



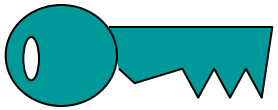
Открытый ключ Васи

Ура! Письмо открылось!

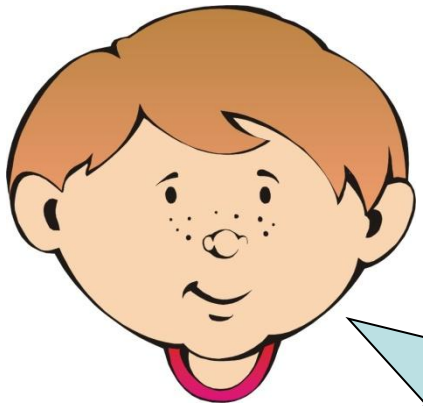




Открытый ключ Васи



Открытый кл



А ключ послать не могу, злодей перехватит…

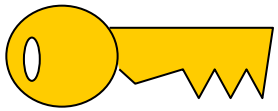
☹

Вася

А у меня нет…

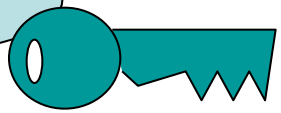
☹

Петя

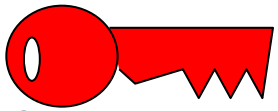


Открытый ключ Васи

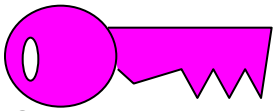
Злодей



Открытый ключ Пети



Закрытый ключ Васи



Закрытый ключ Пети

Асимметричные криптоалгоритмы

Алгоритм RSA (от букв фамилий создателей – Rivest, Shamir, Aldeman)

1.Выбираются два **простых** числа p и q

2.Вычисляется их произведение n=p*q

3.Выбирается произвольное число e (e<n), такое, что *НОД(e,(p-1)(q-1))=1*, то есть e должно быть **взаимно простым** с числом (p-1)(q-1).

4.Методом Евклида решается в **целых числах** уравнение *e*d+(p-1)(q-1)*y=1*. Здесь неизвестными являются переменные d и y

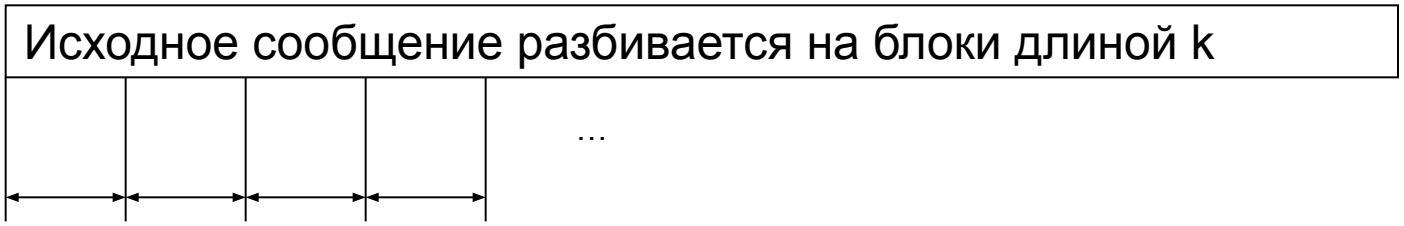
5.Два числа (e,n) – публикуются как **открытый ключ**.

6.Число d хранится в строжайшем секрете – это и есть **закрытый ключ**, который позволит читать все послания, зашифрованные с помощью пары чисел (e,n).

Алгоритм получения ключей для алгоритма RSA

Асимметричные криптоалгоритмы

Алгоритм RSA



Длина блока
$k=[\log_2(n)]$

$\Leftrightarrow$

Число из диапазона
$m_i = (0;2^k-1)$

Вычисляем блоки шифра
$\mathbf{c_i=((m_i)^e)mod\ n}$

Согласно частному случаю теоремы Эйлера:
если число n представимо в виде двух простых чисел p и q, то для любого x имеет место равенство $\mathbf{(x^{(p-1)(q-1)})mod\ n = 1}$

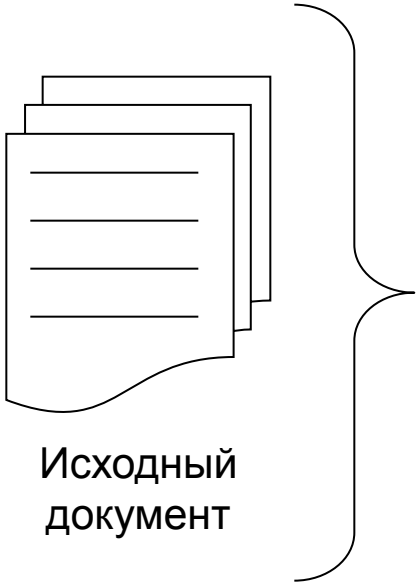
Возведем обе части равенства в степень (-y) : $(x^{(-y)(p-1)(q-1)})\text{mod } n = 1^{(-y)} = 1$.
Теперь умножим обе части на x : $(x^{(-y)(p-1)(q-1)+1})\text{mod } n = 1*x = x$
Согласно алгоритму формирования ключей: $e*d+(p-1)(q-1)*y=1$, или иначе
$\mathbf{e*d=(-y)(p-1)(q-1)+1}$

Следовательно: $\mathbf{(x^{e*d})mod\ n = x}$
Таким образом, для того чтобы прочесть сообщение $c_i=((m_i)^e)\text{mod } n$ достаточно возвести его в степень d по модулю m : $\mathbf{((c_i)^d)mod\ n = ((m_i)^{e*d})mod\ n = m_i}$

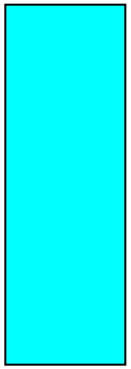
Электронная цифровая подпись

Электронная цифровая подпись (ЭЦП)

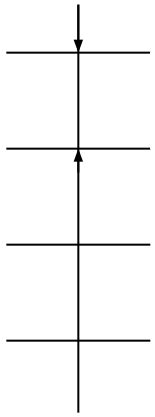
ОТПРАВИТЕЛЬ



Исходный документ



Хеш-сумма (хеш-функция)

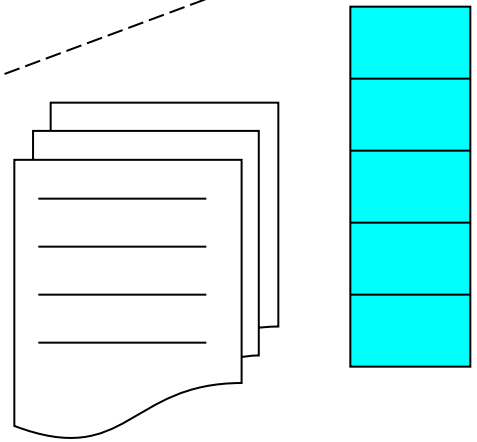


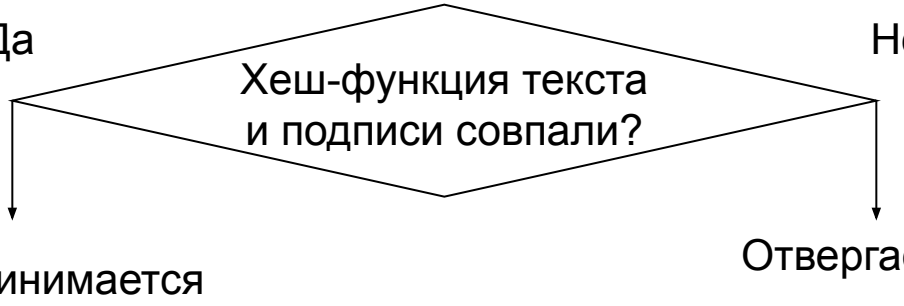
Разбить хеш-сумму на блоки $\mathbf{h}_i$ длиной **k**

$s_i=((h_i)^d)\bmod n$
здесь d – закрытый ключ отправителя

Выполним над полученными блоками операцию
$((s_i)^e)\bmod n = ((h_i)^{d*e})\bmod n = h_{i,}$

(открытый ключ отправителя (e,n) у получателя есть)





ПОЛУЧАТЕЛЬ

Федеральный закон Российской Федерации от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи"

Статья 1. Сфера действия настоящего Федерального закона

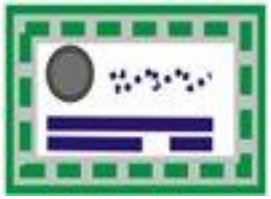
Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Компоненты необходимые для работы с электронной цифровой подписью

Ключевая пара - связанные между собой открытый и закрытый ключ. С помощью закрытого ключа производится подписание документов этот ключ является секретным, доступ к нему должен быть только у владельца ключа. Открытый ключ доступен для всех, с помощью открытого ключа происходит идентификация владельца ЭЦП, т.е. подтверждается владелец электронной цифровой подписи, которой подписан документ. Также открытый ключ используется для шифрования документов.

Ключевой носитель для хранения ключевой пары электронной цифровой подписи – закрытого ключа и открытого ключа. Как правило, это похожий внешне на флэш-диск носитель

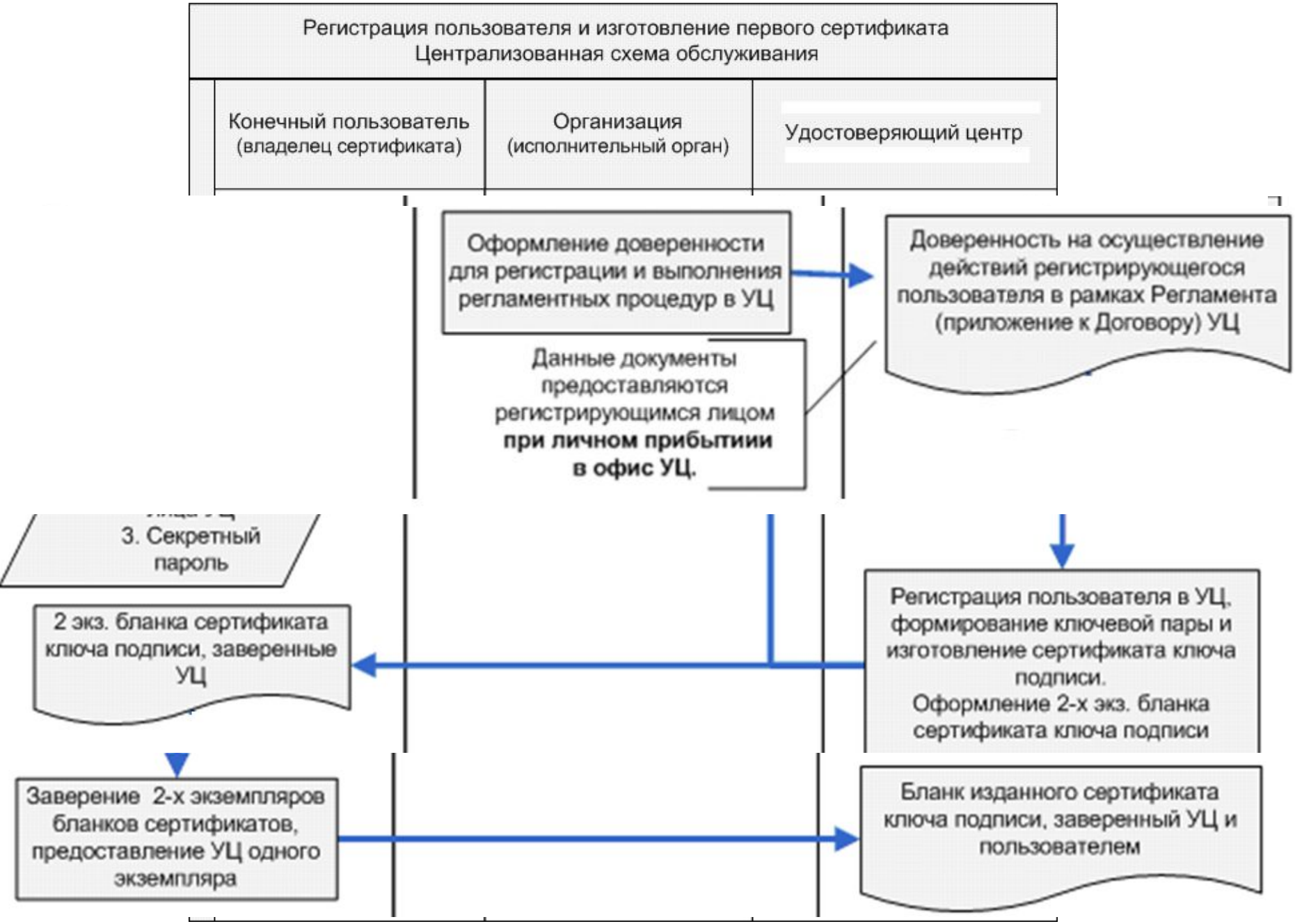
Компоненты необходимые для работы с электронной цифровой подписью



Сертификат открытого ключа подписи.
Сертификаты выпускает уполномоченный удостоверяющий центр (УЦ).
Сертификат подтверждает данные о владельце ЭЦП и его полномочия

Криптопровайдер СКЗИ КриптоПро CSP - программа, предназначенная для формирования и проверки электронной цифровой подписи в соответствии с отечественными стандартами; а также для обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования

Электронная цифровая подпись (ЭЦП)



Фонд социального страхования Российской Федерации

Сертификат ключа подписи

Кому выдан: Иванов Иван Иванович

Кем выдан: Удостоверяющий центр ФСС РФ

Действителен с 26 февраля 2010 г. по 26 февраля 2011 г.

Назначение:
- Подтверждает удаленному компьютеру идентификацию вашего компьютера.
- Защищает сообщения электронной почты.

Версия:	V3
Серийный номер:	01 CA B6 D0 DA 4D B9 20 00 00 00 00 04 4C 00 16
Алгоритм подписи:	ГОСТ Р 34.10/34.11-2001
Издатель:	Псевдоним: УЦ ФСС РФ Должность: Уполномоченное лицо УЦ ФСС РФ Подразделение: Удостоверяющий центр ФСС РФ Организация: Центральный аппарат Фонда социального страхования РФ Электронная почта: info-uc@fss.ru Почтовый адрес: 107139, Орликов переулок, дом 3А Город: Москва Страна: RU
Действителен с:	26 февраля 2010 г. 13:49:08 (GMT+03:00)

Издатель:	Псевдоним: УЦ ФСС РФ Должность: Уполномоченное лицо УЦ ФСС РФ Подразделение: Удостоверяющий центр ФСС РФ Организация: Центральный аппарат Фонда социального страхования РФ Электронная почта: info-uc@fss.ru Почтовый адрес: 107139, Орликов переулок, дом 3А Город: Москва Страна: RU
Действителен с:	26 февраля 2010 г. 13:49:08 (GMT+03:00)
Действителен по:	26 февраля 2011 г. 13:49:08 (GMT+03:00)
Владелец:	Имя: Иванов Иван Иванович Должность: Инженер Подразделение: Ремонтное локомотивное депо Великолукское Организация: Октябрьская железная дорога филиала ОАО "РЖД" Почтовый адрес: 182100, г. Великие Луки, ул. Угольная, д. 1 Область: Псковская область Город: Великие Луки Страна: RU Неструктурированное имя: Тестовый сертификат ИНН: 7708503727 РНС ФСС: 6000004463 КП ФСС: 6000
Открытый ключ:	ГОСТ Р 34.10-2001 (512 бит) 04 40 82 9B 1C 9C C7 3B 42 07 F9 45 D7 FA 9E 6A 4D 3E 4A BA 3E 07 30 ED B3 14 F8 0E 1D CF 3E F9 5E 08 AC A8 E3 AD 01 F1 F7 94 81 70 6B 3E 05 FB 99 FE AD EF 9F 44 C2 E3 B0 3F 5D A3 6E DF 42 48 22 FC

Расширения сертификата X.509

Использование ключа:	Цифровая подпись, Неотрекаемость, Шифрование ключей, Шифрование данных, Согласование ключей (F8)

Расширенное использование ключа:	Проверка подлинности клиента (1.3.6.1.5.5.7.3.2) Защищенная электронная почта (1.3.6.1.5.5.7.3.4)
Точки распространения списков отзыва (CRL):	[1]Точка распространения списка отзыва (COC): Имя точки распространения: Полное имя: URL=http://www.fss.ru/uc/CA_FSS_RF_2010.crl
Доступ к информации о центрах сертификации:	[1]Доступ к сведениям центра сертификации Метод доступа=Поставщик центра сертификации (1.3.6.1.5.5.7.48.2) Дополнительное имя: URL=http://www.fss.ru/uc/CA_FSS_RF_2010.cer
Идентификатор ключа субъекта:	17 37 70 06 92 B2 9B AD EE 50 3E 34 52 B8 19 F0 A7 F4 A2 76
Идентификатор ключа центра сертификатов:	Идентификатор ключа=5F 75 7C 3D 30 28 DE EB 55 A6 60 C9 21 C3 FA 81 24 80 FC 85
Основные ограничения:	Тип субъекта=Пользователь

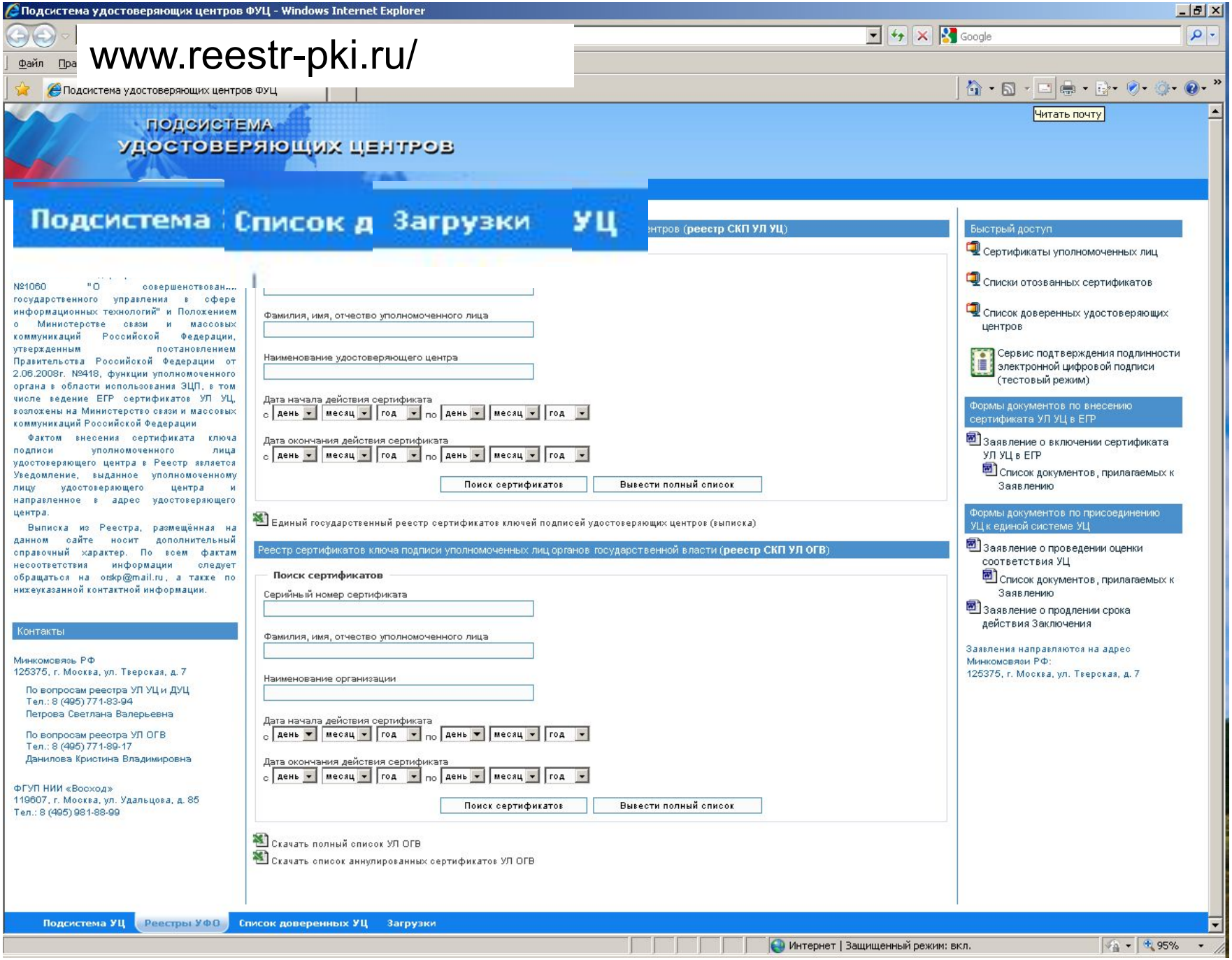
Результат проверки сертификата

Сертификат действителен.
Проверен 27 февраля 2010 г. 14:45:22 (GMT+03:00).

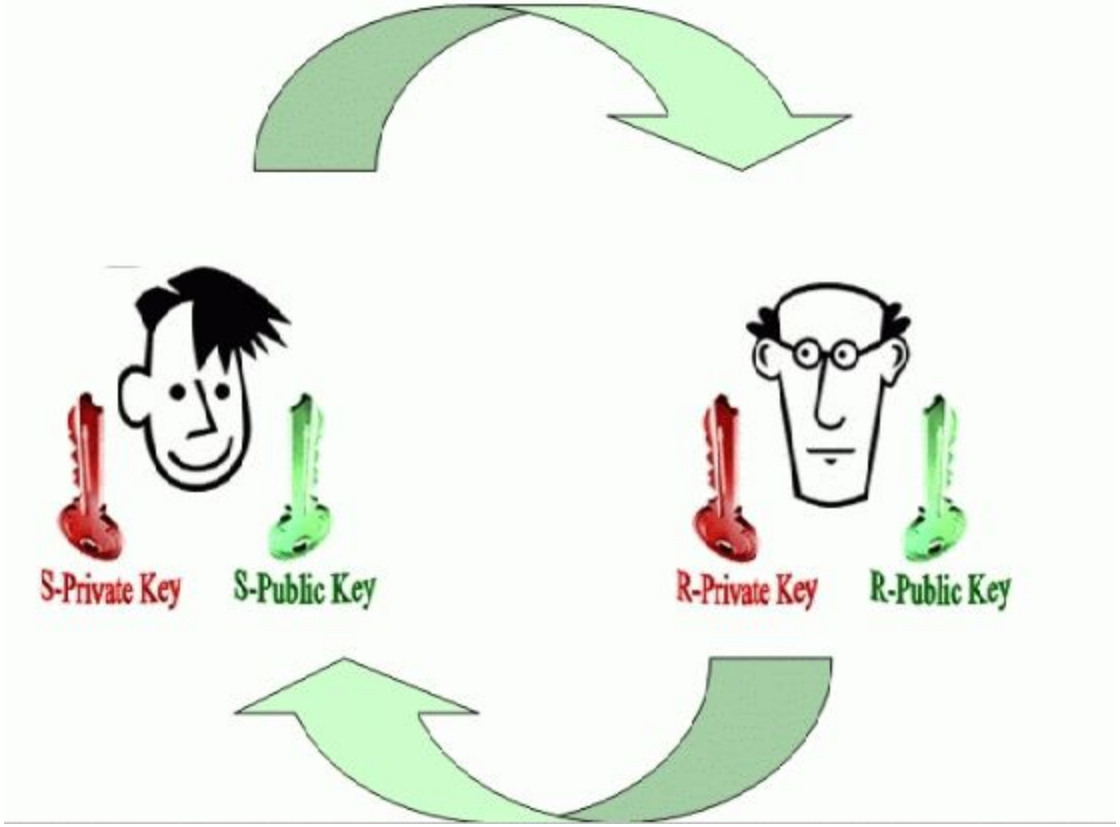
Подпись уполномоченного лица и печать Удостоверяющего Центра

_____ / _____/

«___» _____ 200__ г.

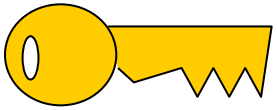

Подсистема удостоверяющих центров ФУЦ - Windows Internet Explorer
www.reestr-pki.ru/
Подсистема удостоверяющих центров ФУЦ
Читать почту
ПОДСИСТЕМА
УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ
Подсистема
Список д
Загрузки
УЦ
№1060 "О совершенствован... государственного управления в сфере информационных технологий" и Положением о Министерстве связи и массовых коммуникаций Российской Федерации, утвержденным постановлением Правительства Российской Федерации от 2.06.2008г. №418, функции уполномоченного органа в области использования ЭЦП, в том числе ведение ЕГР сертификатов УЛ УЦ, возложены на Министерство связи и массовых коммуникаций Российской Федерации
Фактом внесения сертификата ключа подписи уполномоченного лица удостоверяющего центра в Реестр является Уведомление, выданное уполномоченному лицу удостоверяющего центра и направленное в адрес удостоверяющего центра.
Выписка из Реестра, размещённая на данном сайте носит дополнительный справочный характер. По всем фактам несоответствия информации следует обращаться на otskp@mail.ru, а также по нижеуказанной контактной информации.
Контакты
Минкомсвязь РФ
125375, г. Москва, ул. Тверская, д. 7
По вопросам реестра УП УЦ и ДУЦ
Тел.: 8 (495) 771-83-94
Петрова Светлана Валерьевна
По вопросам реестра УП ОГВ
Тел.: 8 (495) 771-89-17
Данилова Кристина Владимировна
ФГУП НИИ «Восход»
119607, г. Москва, ул. Удальцова, д. 85
Тел.: 8 (495) 981-88-99
нтров (реестр СКП УЛ УЦ)
Фамилия, имя, отчество уполномоченного лица
Наименование удостоверяющего центра
Дата начала действия сертификата
с день месяц год по день месяц год
Дата окончания действия сертификата
с день месяц год по день месяц год
Поиск сертификатов
Вывести полный список
Единый государственный реестр сертификатов ключей подписей удостоверяющих центров (выписка)
Реестр сертификатов ключа подписи уполномоченных лиц органов государственной власти (реестр СКП УЛ ОГВ)
Поиск сертификатов
Серийный номер сертификата
Фамилия, имя, отчество уполномоченного лица
Наименование организации
Дата начала действия сертификата
с день месяц год по день месяц год
Дата окончания действия сертификата
с день месяц год по день месяц год
Поиск сертификатов
Вывести полный список
Скачать полный список УЛ ОГВ
Скачать список аннулированных сертификатов УЛ ОГВ
Быстрый доступ
Сертификаты уполномоченных лиц
Списки отозванных сертификатов
Список доверенных удостоверяющих центров
Сервис подтверждения подлинности электронной цифровой подписи (тестовый режим)
Формы документов по внесению сертификата УЛ УЦ в ЕГР
Заявление о включении сертификата УЛ УЦ в ЕГР
Список документов, прилагаемых к Заявлению
Формы документов по присоединению УЦ к единой системе УЦ
Заявление о проведении оценки соответствия УЦ
Список документов, прилагаемых к Заявлению
Заявление о продлении срока действия Заключения
Заявления направляются на адрес Минкомсвязи РФ:
125375, г. Москва, ул. Тверская, д. 7
Подсистема УЦ
Реестры УФО
Список доверенных УЦ
Загрузки
Интернет | Защищенный режим: вкл.
95%

Распространение открытых ключей

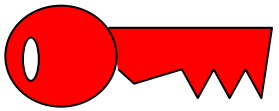


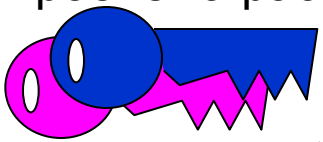
Проблема распространения открытых ключей

Открытый ключ Васи



Открытый ключ Пети

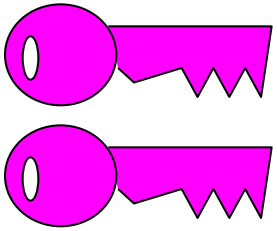




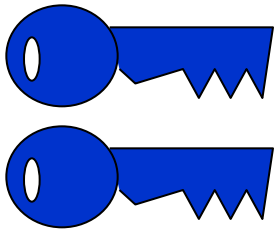
Вася

Петя

Ключи Злодея для Васи

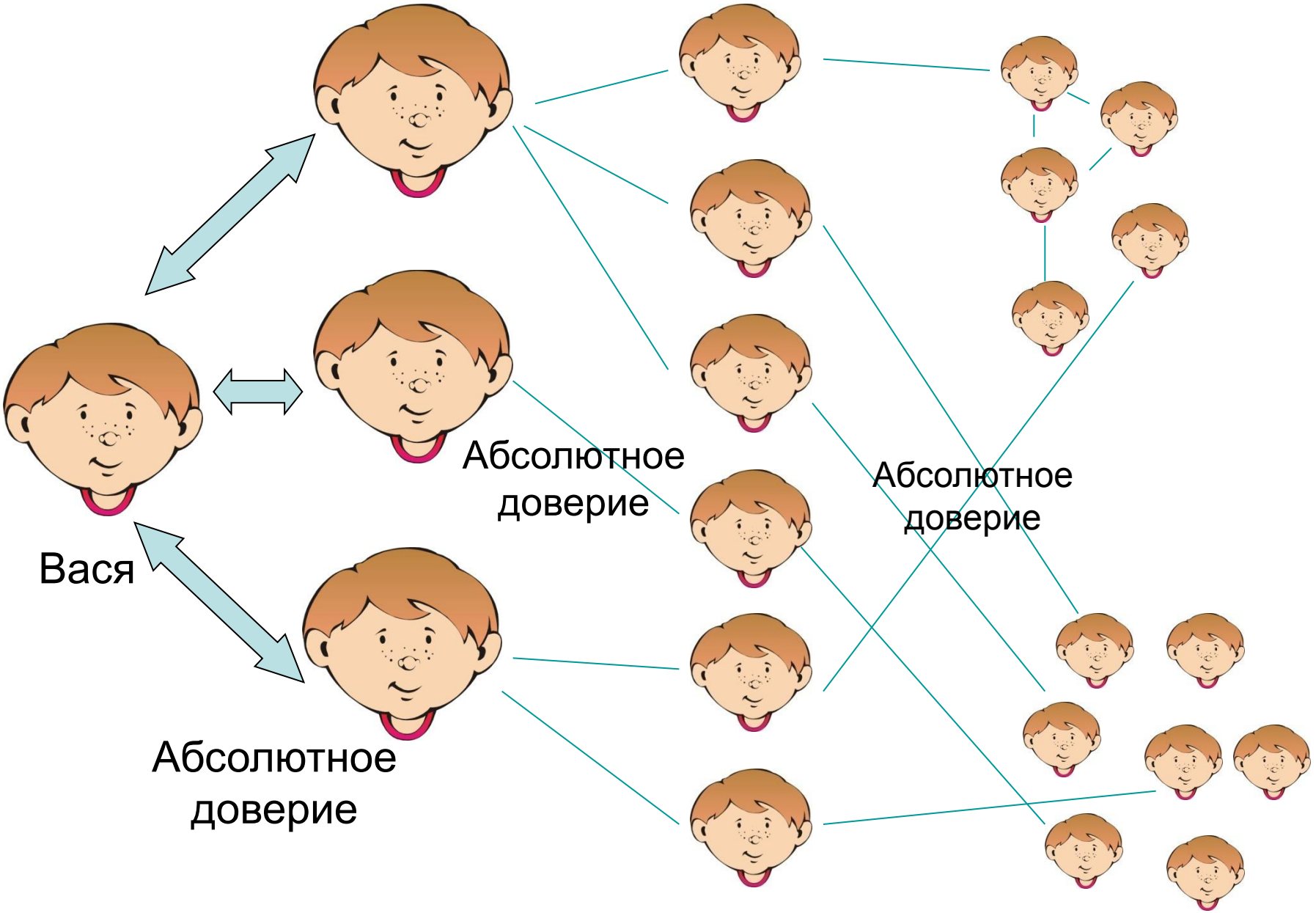


Злодей

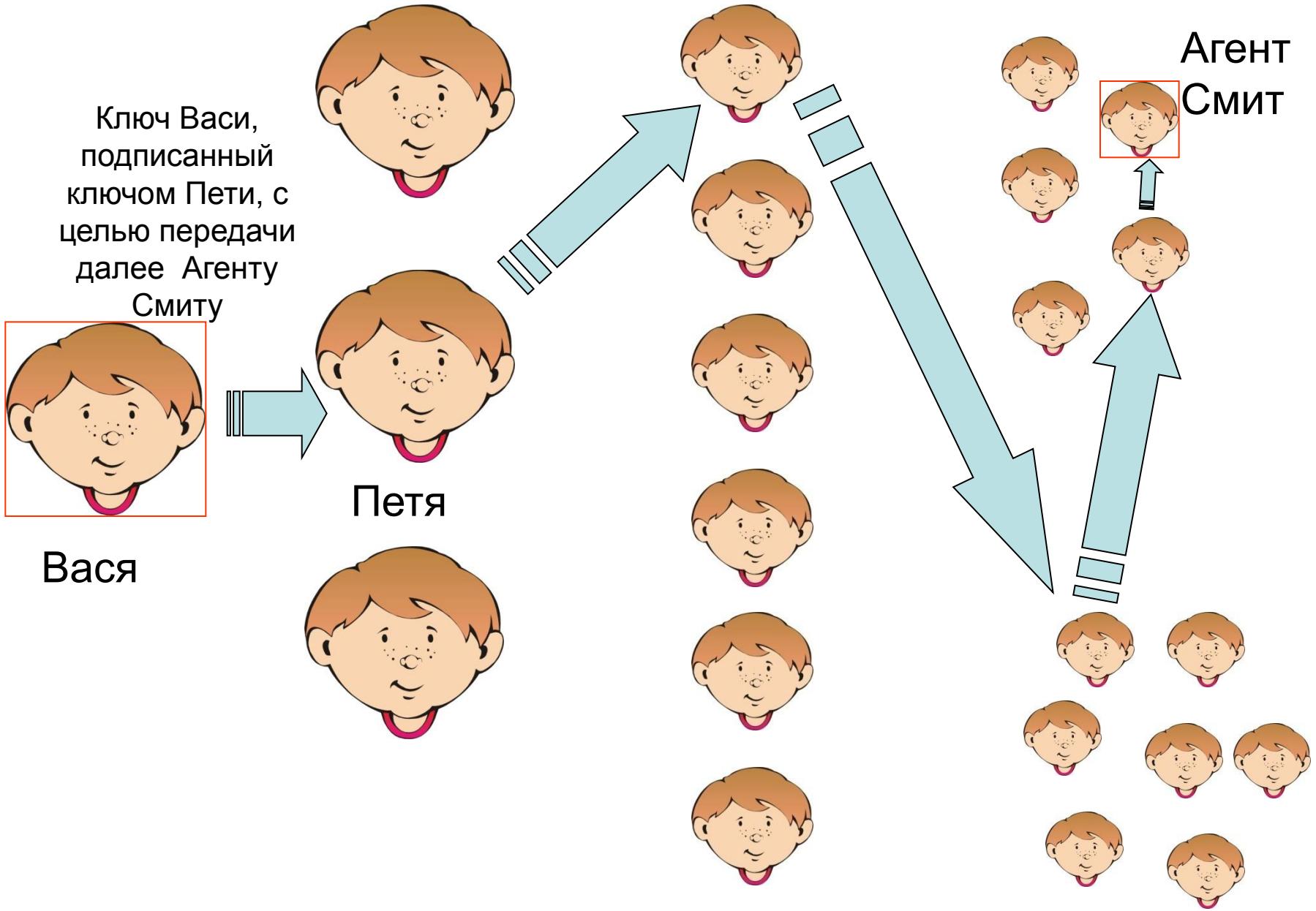


Ключи Злодея для Пети

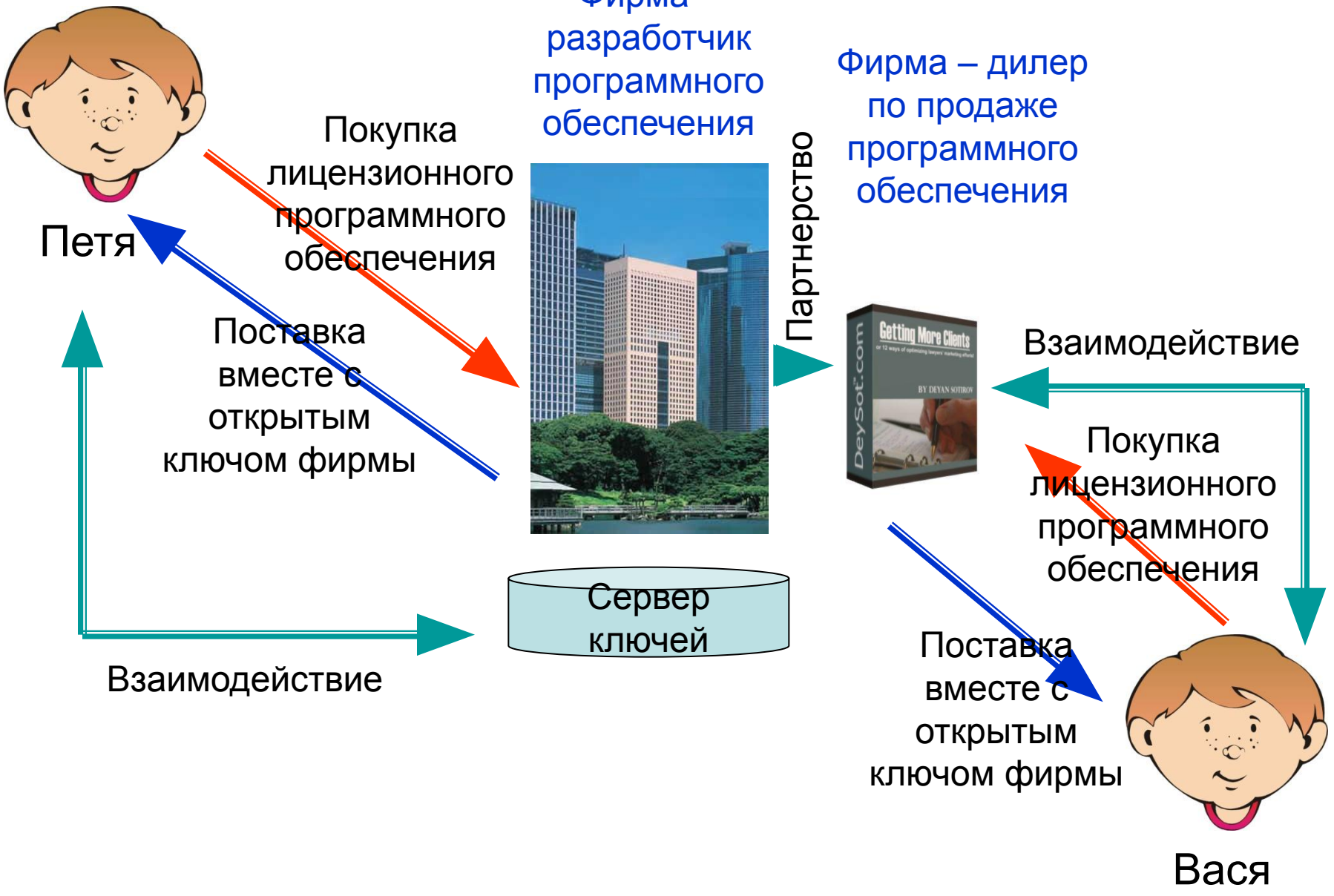
Проблема распространения открытых ключей



Проблема распространения открытых ключей



Проблема распространения открытых ключей



Открытый ключ, подписанный какой-либо третьей стороной, **называется заверенным с помощью сертификата**.

Сертификатом называется информационный пакет, содержащий какой-либо объект (обычно ключ) и электронную подпись, подтверждающую этот объект от имени чьего-либо лица

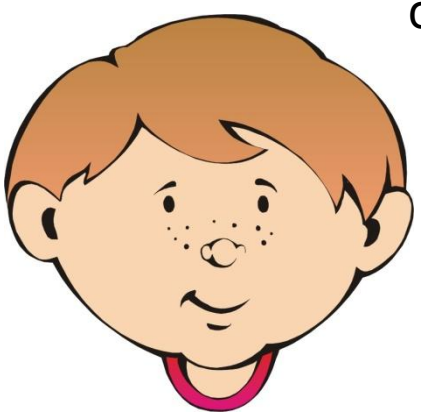
Проблема распространения открытых ключей

Возьмем числа a, b

Согласен

Я получил случайное число X

Я получил случайное число Y



Я вычислил $a^X \bmod b$

Я вычислил $a^Y \bmod b$

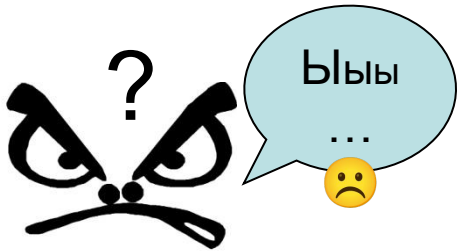
Вычисляю $(a^Y \bmod b)^X \bmod b$

Вычисляю $(a^X \bmod b)^Y \bmod b$

Вася

Петя

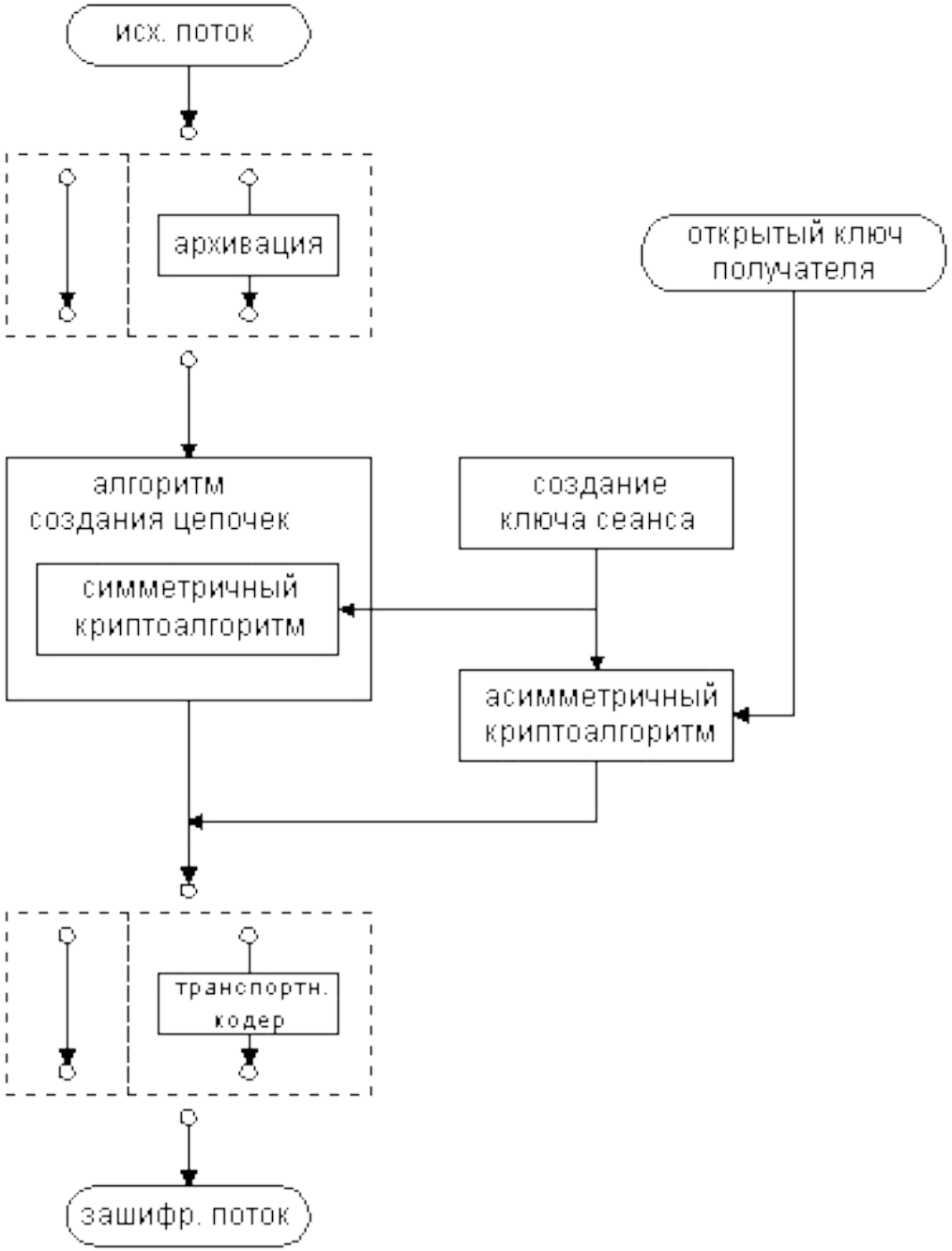
Получилось уникальное число $a^{XY} \bmod b$



Злодей

Получилось уникальное число $a^{XY} \bmod b$

:) Второе краткое резюме :)



Общая схема асимметричной криптосистемы

Аутентификация пользователя

Способы аутентификации пользователя

Пароль «Мама мыла раму*!*»

Основными характеристиками устройств аутентификации являются:

1. частота ошибочного отрицания законного пользователя;
2. частота ошибочного признания постороннего;
3. среднее время наработки на отказ;
4. число обслуживаемых пользователей;
5. стоимость;
6. объем информации, циркулирующей между считывающим устройством и блоком сравнения;
7. приемлемость со стороны пользователей.

Защита программного обеспечения

Основные положения по разработке безопасного программного обеспечения

1. не используйте экзотические и недокументированные возможности языка программирования : Вы не уверены в том, как они реализуются на самом деле

2. оформляйте исходный текст ясно и четко, используйте необходимые комментарии

3. используйте скобки для явного указания порядка операций : компилятор может оптимизировать выполнение выражений и начать, скажем, сложение F(1)+F(2)+F(3) со второго знака "+", тем самым вызвав сначала функцию F от 2, затем от 3, а только затем от 1 – если в функции изменяются какие-либо глобальные переменные это может привести к непредсказумым последствиям

4. при всех удобных случаях используйте передачу параметров функции в качестве аргументов, а не в глобальных переменных

5. используйте структурное программирование : разбивайте сложные блоки кода на процедуры с ясной структурой и легко контролируемым набором параметров

6. никогда не программируйте недокументированные возможнности : технология "reverse engineering" – дизассемблирование и обратная компиляция" – на сегодняшний день достигла огромных результатов, особенно в отношении высокоуровневых языков программирования

7. закрывайте файлы сразу же по окончании работы с ними, а если Вы записываете важную информацию в течение долгого времени – периодически вызывайте функции сброса файлового буфера на дисковый накопитель

8. проверяйте свободное место на диске перед записью в файл : некоторые операционные выдают ошибки при записи на переполненный диск нестандартным образом, результат этого может быть плачевным

9. блокируйте файлы и наборы данных, если Вы обращаетесь к ним по записи из нескольких параллельно работающих процессов или программ

10. старайтесь как можно сильнее сократить время записи в совместно используемые файлы, а, следовательно, и время их блокирования

11. не будьте заранее уверенными, что программа запущена из той директории, где расположен ее исполнимый файл, – одной из первых команд после запуска программы явно смените каталог на желаемый

12. при работе с внешними и сетевыми устройствами и дисками стройте циклы ожидания таким образом, чтобы из них был возможен выход по истечении определенного периода ожидания ответа – тайм-аута

13. очень тщательно разрабатывайте схему синхронизации параллелльно работающих с одними и теми же данными процессов

тщательно проверяйте алгоритмы на синдром "мертвой петли" – это ситуация, когда процесс А, начав изменять объект 1 и заблокировав его в связи с этим, ожидает снятия блокирования с объекта 2, в то время как процесс В, в то же самое время начавший изменять объект 2 и заблокировав его, ожидает снятия блокировки с объекта 1 – подобная проблема при такой схеме синхронизации теоретически неразрешима, единственный выход из нее – рассматривать объекты 1 и 2 как единое целое с возможностью только совместной блокировки

14. аккуратно выделяйте и очищайте объекты в динамической памяти

15. при необходимости используйте криптографию

16. никогда не передавайте пароль открытым текстом

17. используйте криптостойкие алгоритмы шифрования и хеширования

18. вычищайте блоки оперативной памяти после того как информация (пароли, ключи, конфиденциальные данные), находившаяся в них, стала ненужной

19. всегда проверяйте длины строк и массивов перед началом работы с ними

20. встраивайте в Ваши системы требование регистрации каждого оператора с уникальным паролем и записью как можно большего количества информации о сеансе в лог-файл, недоступный для изменения операторам

21. тщательно тестируйте Ваши приложения, в том числе на больших и неправильных входных данных

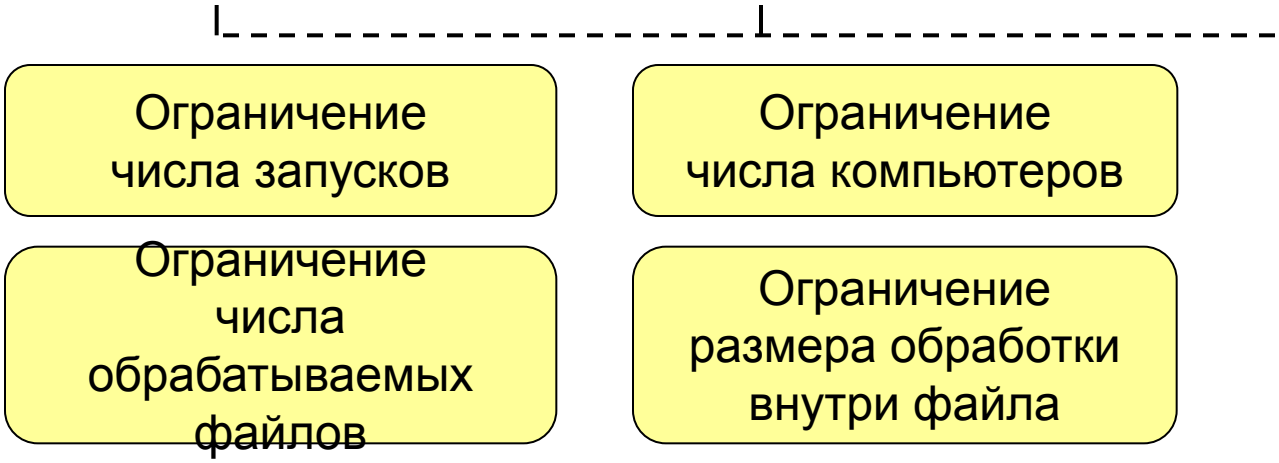
Противодействие изучению исходного кода

- Абстрагирование от языка реализации
- Динамическое ветвление
- Контекстная зависимость
- Разнотипные данные (хуки), инструкции препроцессору
- Использование многопоточности

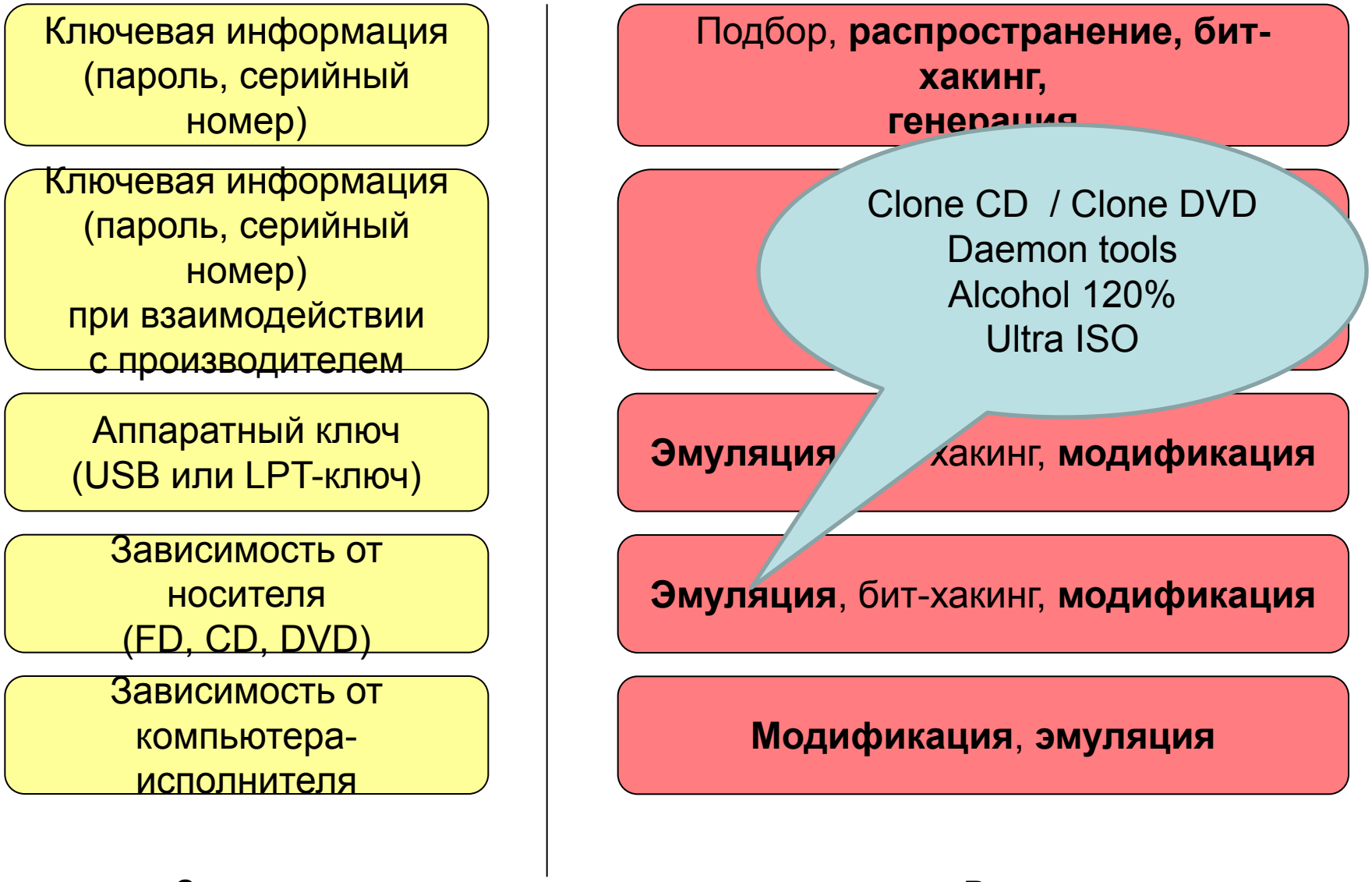
Противодействие изучению двоичного кода

- Защита от дизассемблирования
  - Архивация
  - Шифрование
  - Самогенерация кодов
  - Обман дизассемблера
- Защита от трассировки
  - Обнаружение присутствия программ-трассировщиков
  - Обнаружение воздействия на программу процесса трассировки

Защита программного обеспечения от несанкционированного распространения

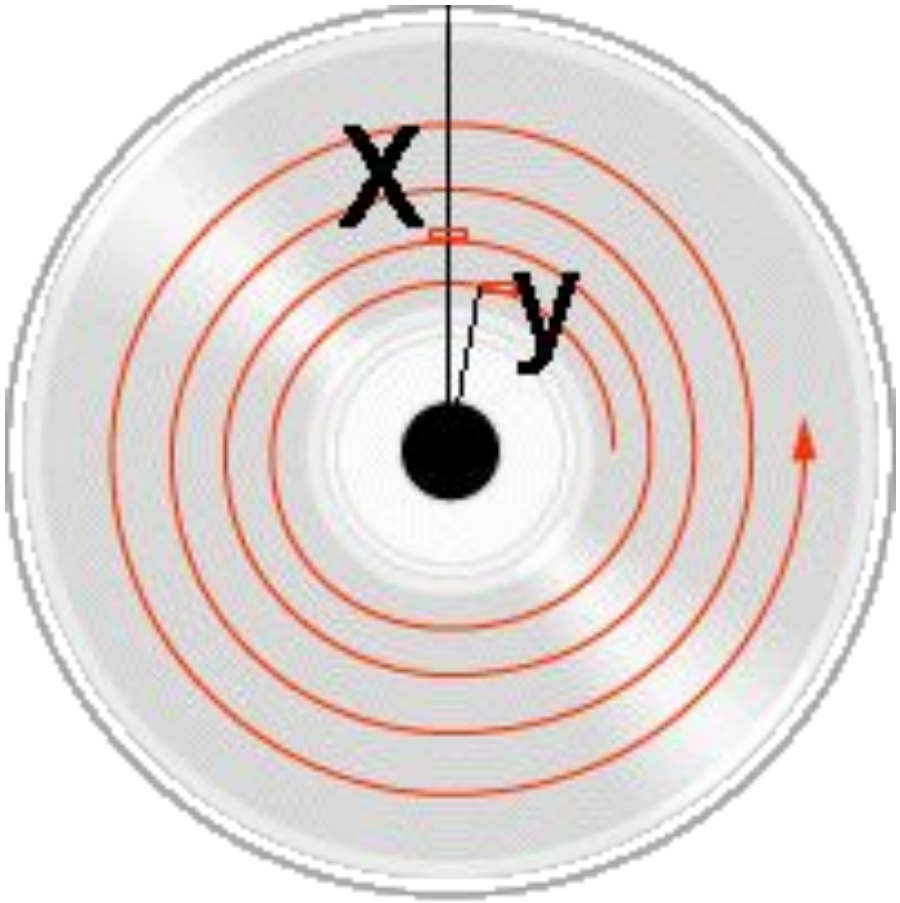


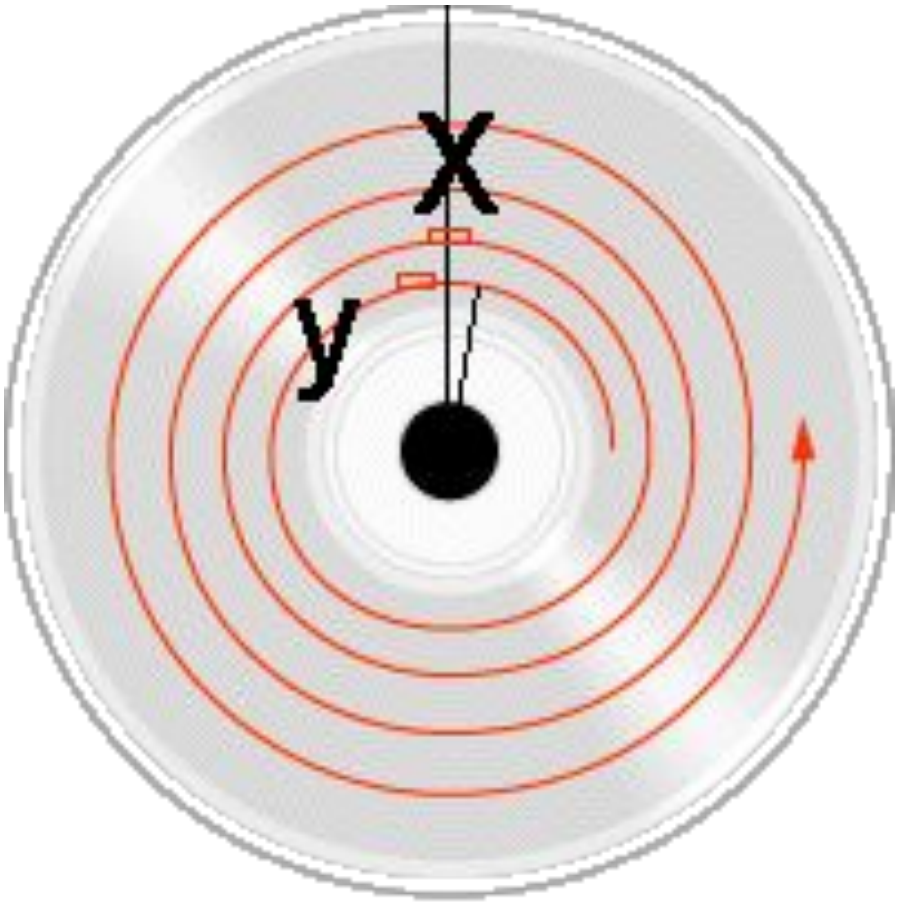
Защита программного обеспечения от несанкционированного распространения



Аппаратные ключи

Измерение угла между секторами





Раздел третий

«Сетевая безопасность»

Получение доступа к информации

Получение несанкциониро ванного доступа к услугам

Вывод из рабочего режима определенног о класса услуг

Вспомогатель ный этап другой более крупной атаки

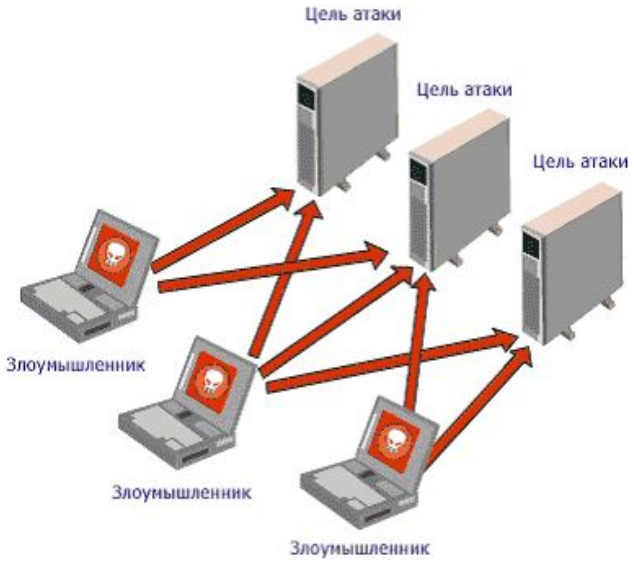
Основные цели атак на серверное оборудование

Сетевая безопасность

«Один к одному»

«Один ко многим»

«Многие к одному»

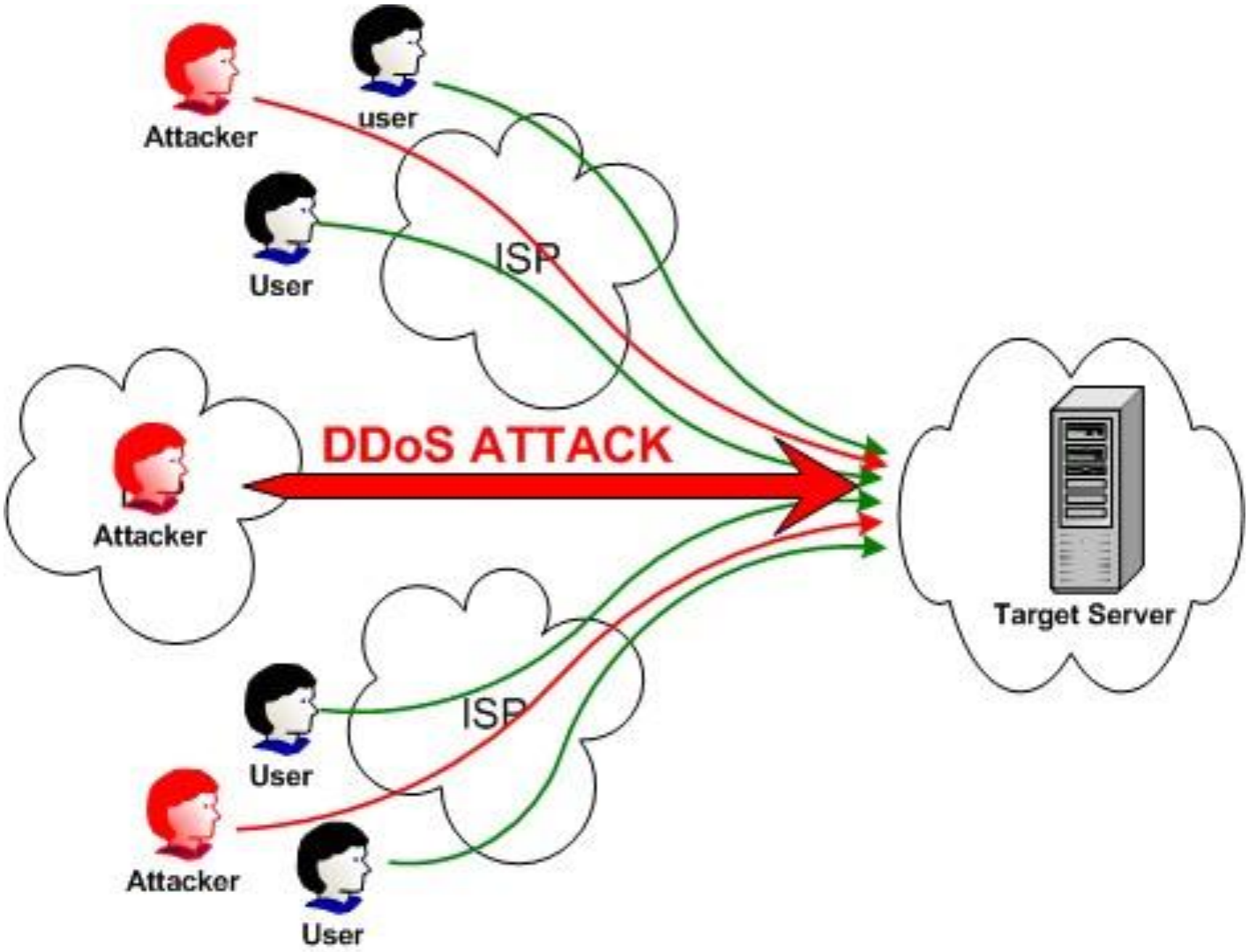


«Многие ко многим»

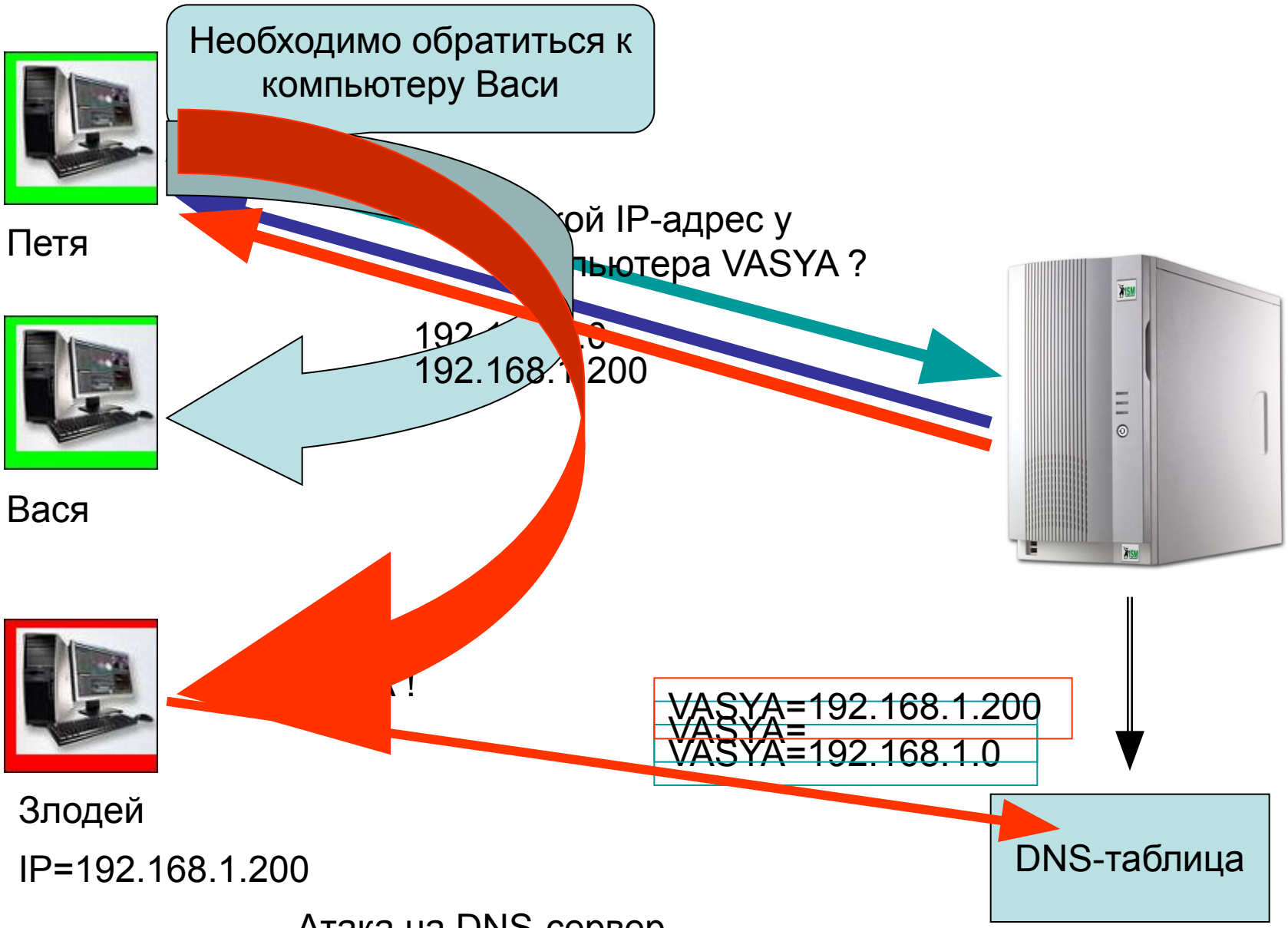
Сетевая безопасность

DoS атака – Denial of Service, дословно – «Отказ в обслуживании»

DDoS атака – Distributed DoS, – «Распределенная DoS атака»

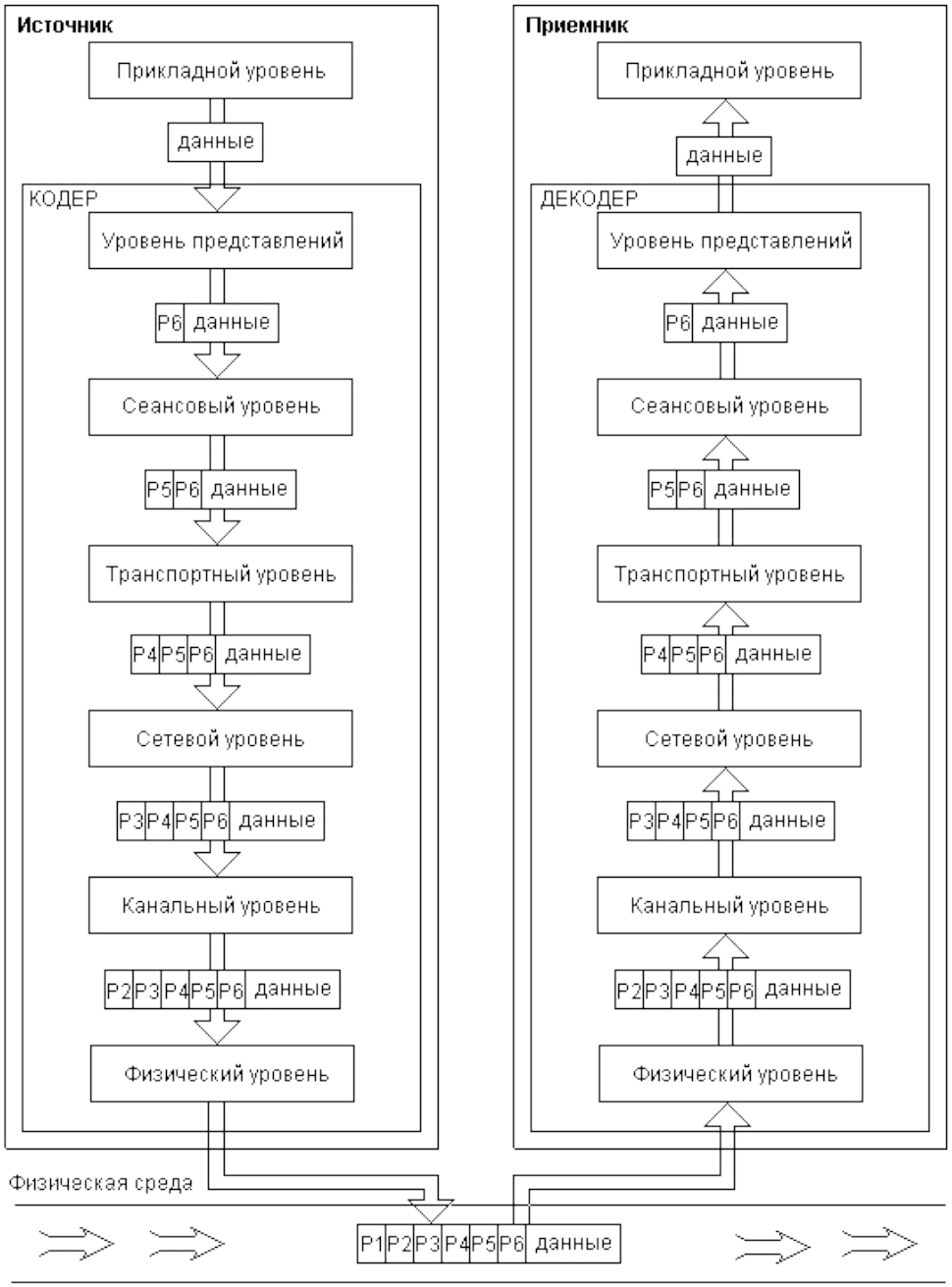


Сетевая безопасность



Атака на DNS-сервер

Сетевая безопасность



Семиуровневая модель OSI

Эталонная модель взаимодействия открытых систем OSI (англ. Open Systems Interconnection) была разработана институтом стандартизации ISO с целью разграничить функции различных протоколов в процессе передачи информации от одного абонента другому. Подобных классов функций было выделено 7 – они получили название уровней. Каждый уровень выполняет свои определенные задачи в процессе передачи блока информации, причем соответствующий уровень на приемной стороне производит преобразования, точно обратные тем, которые производил тот же уровень на передающей стороне. В целом прохождение блока данных от отправителя к получателю показано на рисунке. Каждый уровень добавляет к пакету небольшой объем своей служебной информации – префикс (на рисунке они изображены как P1...P7). Некоторые уровни в конкретной реализации вполне могут отсутствовать.

Сетевая безопасность

DoS-атаки на уровнях сетевой модели

Физический уровень

- Постановка шумов по полосе пропускания канала связи

Канальный уровень

- Сбой синхропосылок
- Передача данных «без разрешения и не в свое время»

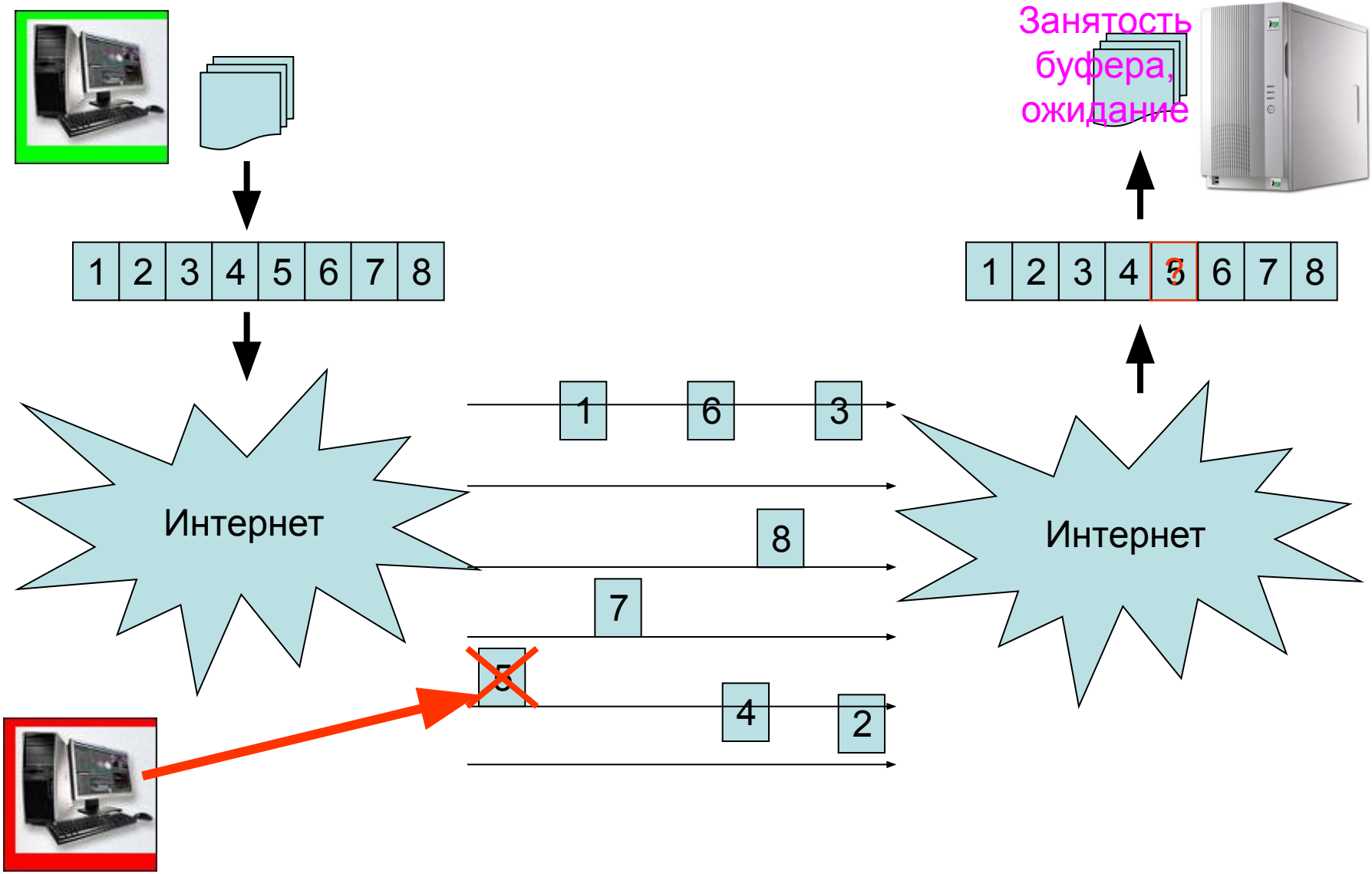
Сетевой уровень

- Атаки на протокол IP
- Атаки путем заведомо неправильной маршрутизации

Сетевая безопасность

DoS-атаки на уровнях сетевой модели

Транспортный уровень



Сетевая безопасность

DoS-атаки на уровнях сетевой модели

Сеансовый уровень

Атака SYN-Flood

SYN

SYN, ACK

ACK

Буфер подключений

Доступ невозможен

Таймаут, разрыв

??????????

(а мы ничего не просили…)

SYN (указан обратный несуществующий или любой сторонний адрес)

Схема реализации угрозы
«Анализ сетевого трафика»

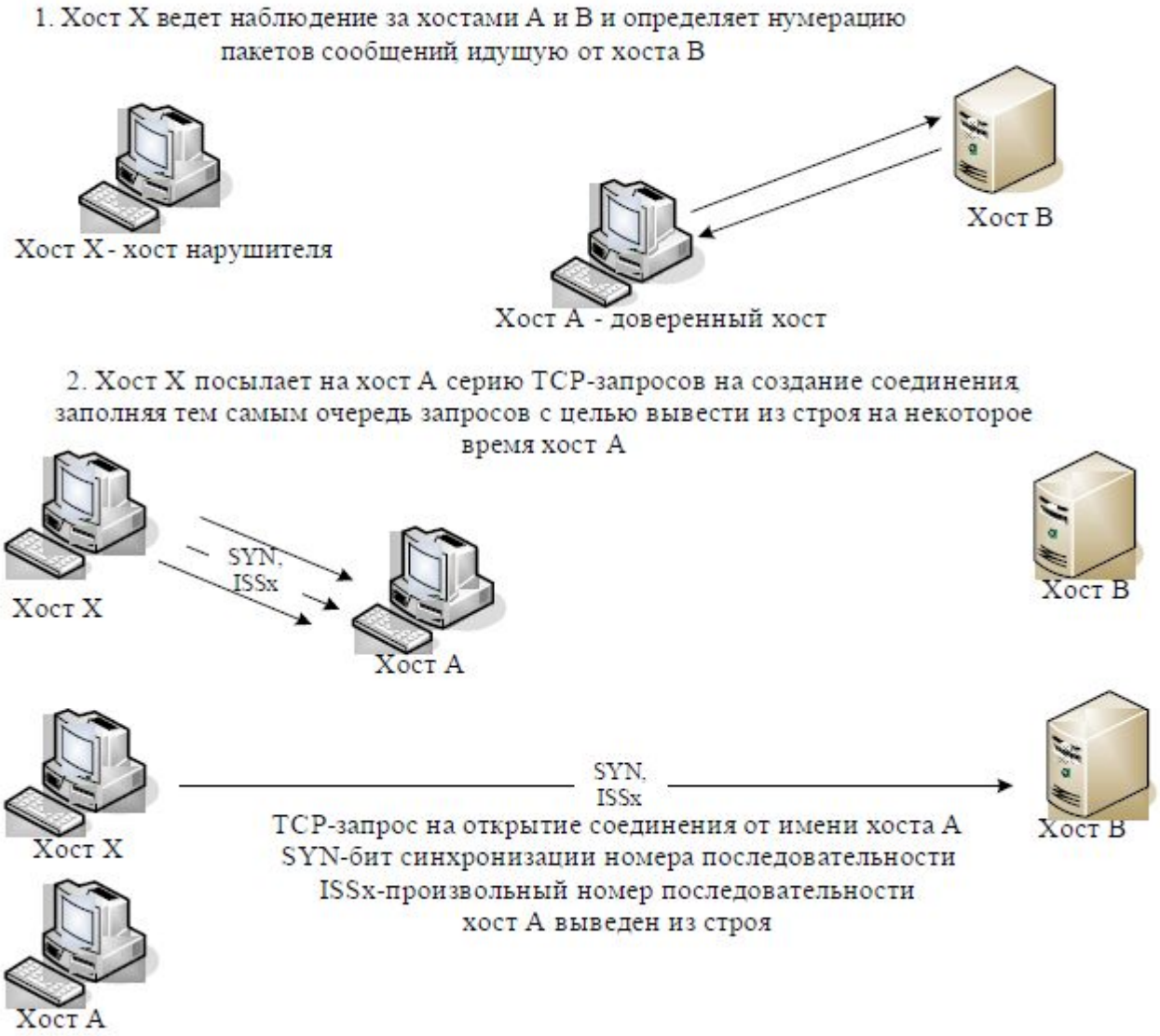


Схема реализации угрозы
«Подмена доверенного объекта сети» (начало)

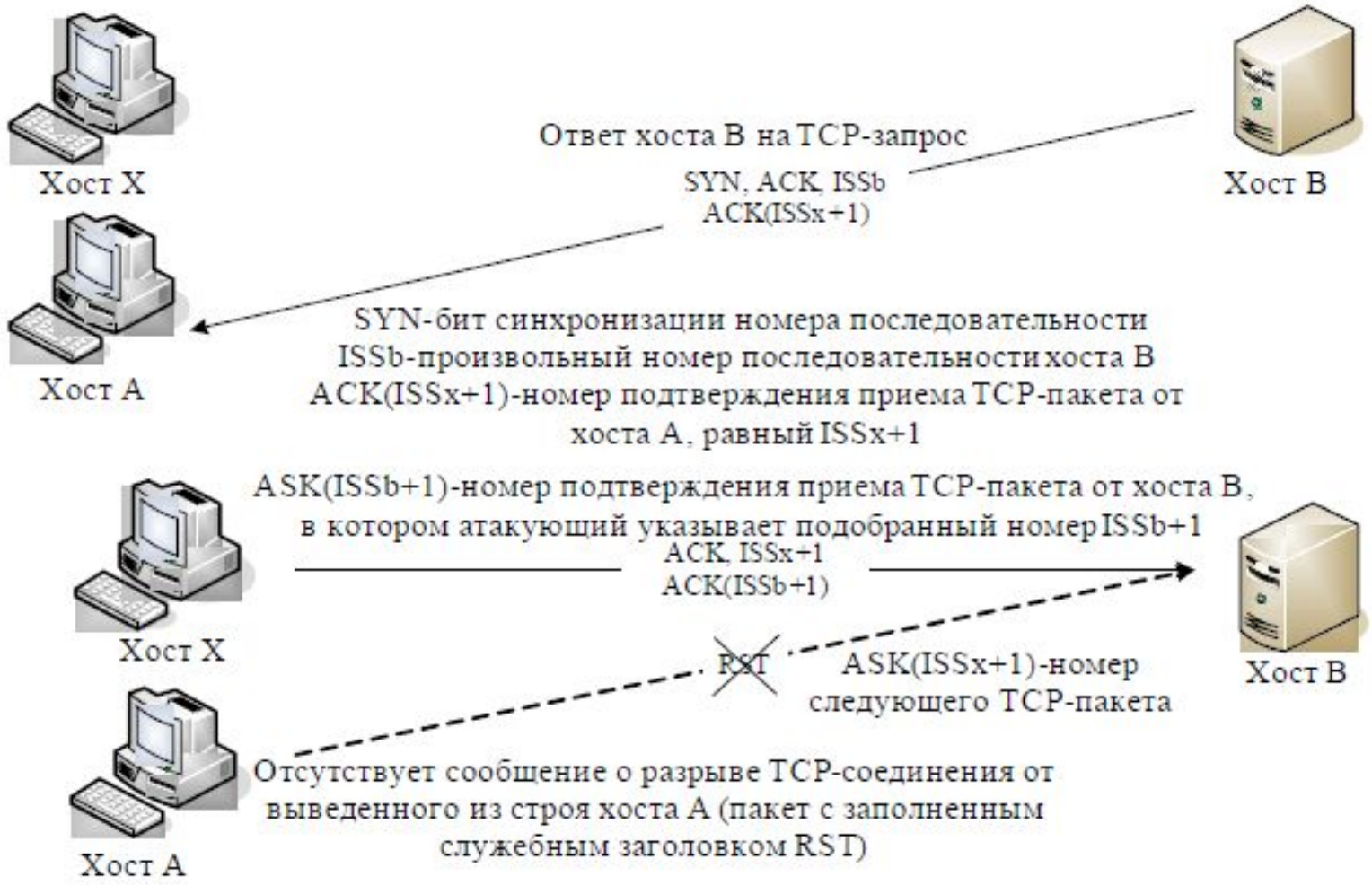


Схема реализации угрозы
«Подмена доверенного объекта сети» (окончание)

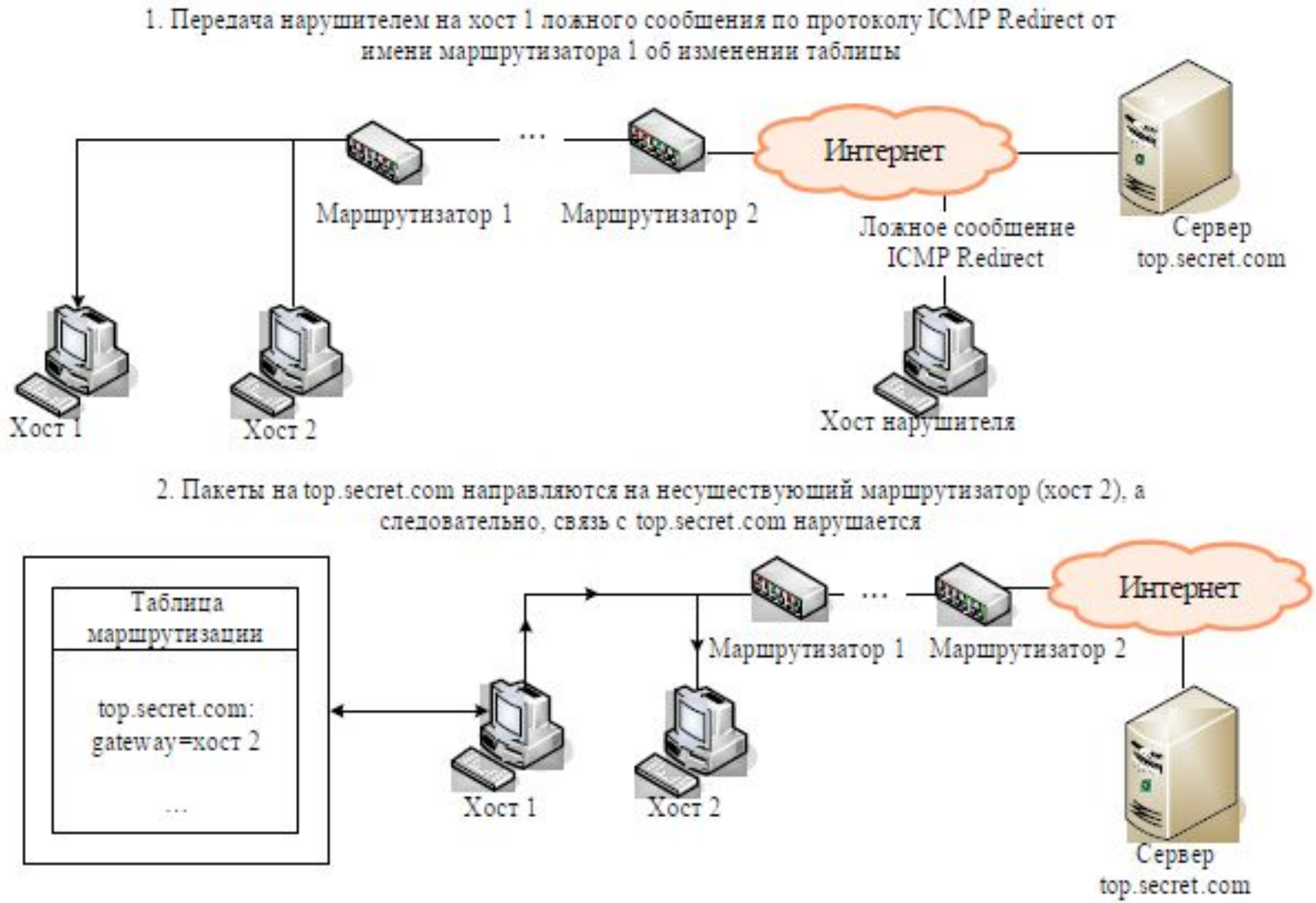


Схема реализации атаки «Навязывание ложного маршрута» (внутрисегментное)

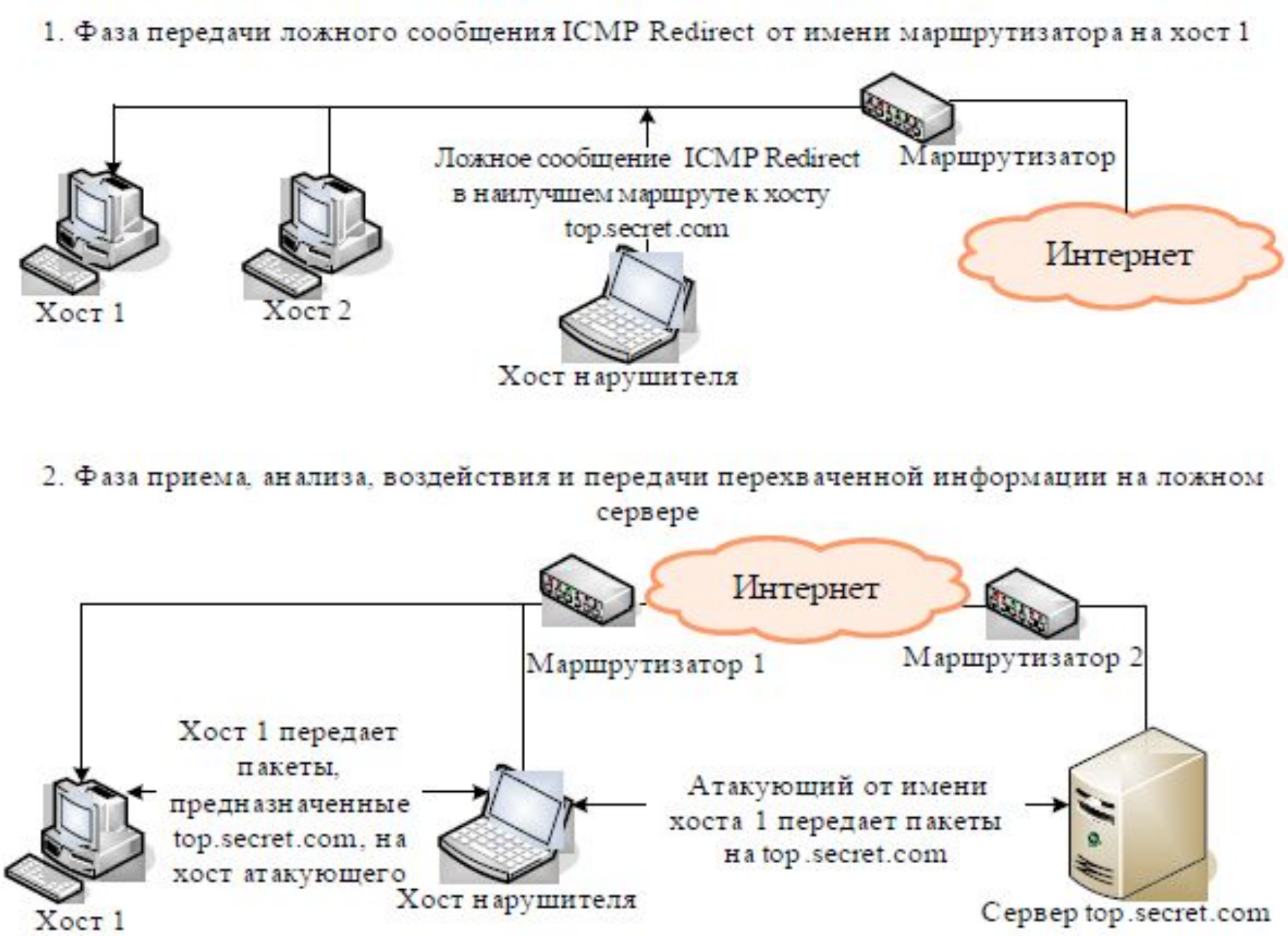


Схема реализации атаки «Навязывание ложного маршрута» (межсегментное)

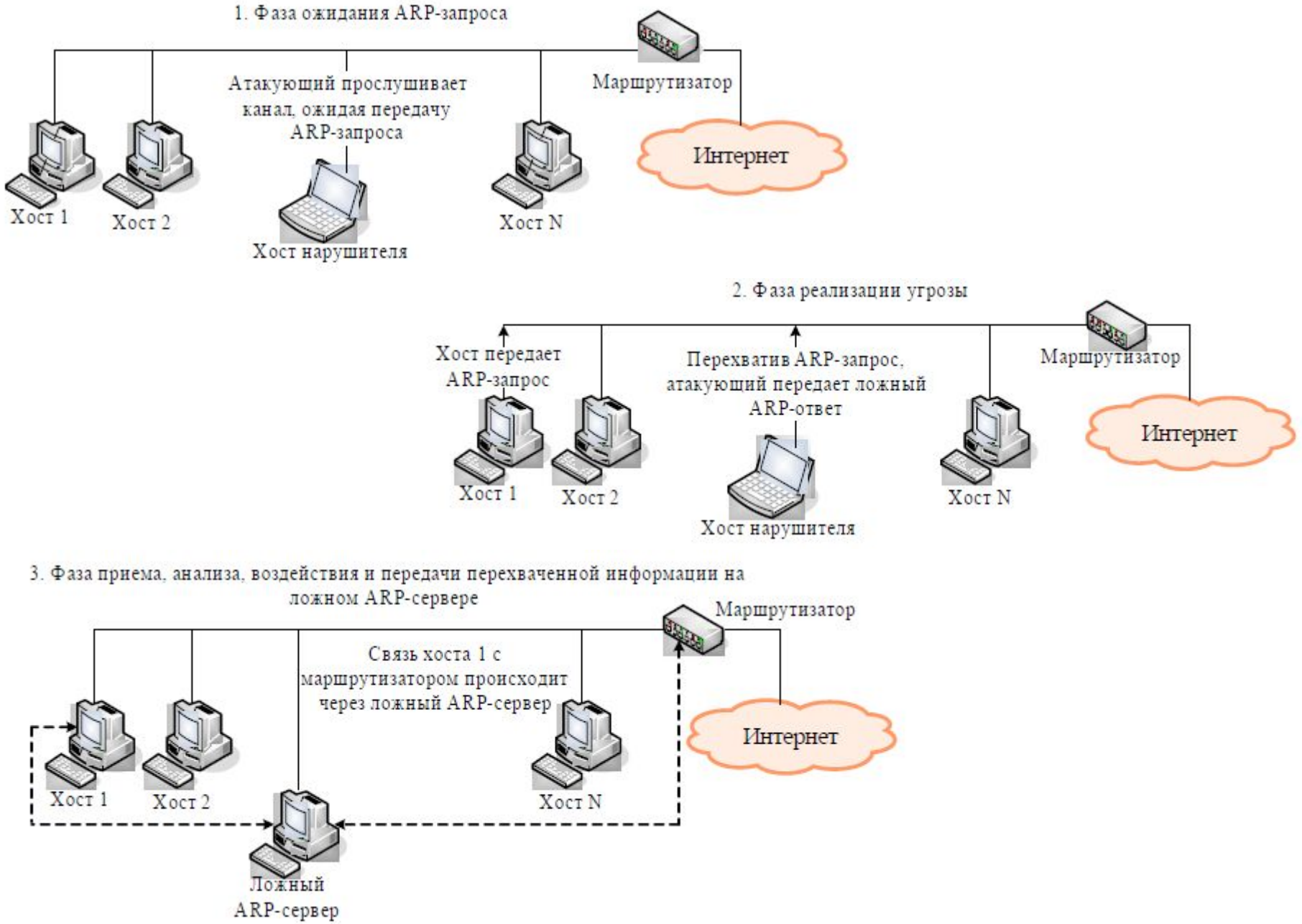


Схема реализации угрозы «Внедрение ложного ARP-сервера»

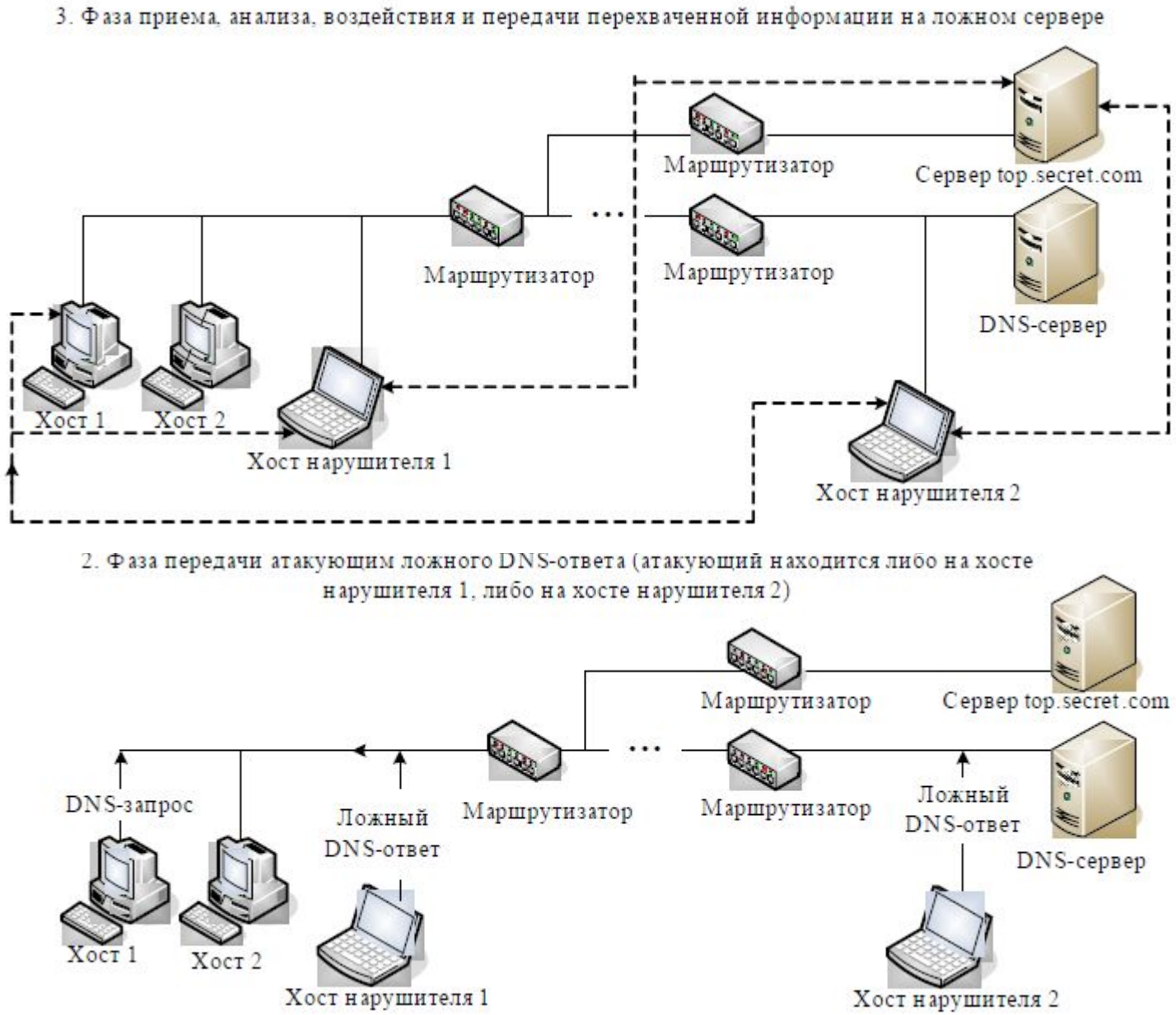


Схема реализации угрозы «Внедрение ложного DNS-сервера» путем перехвата DNS-запроса

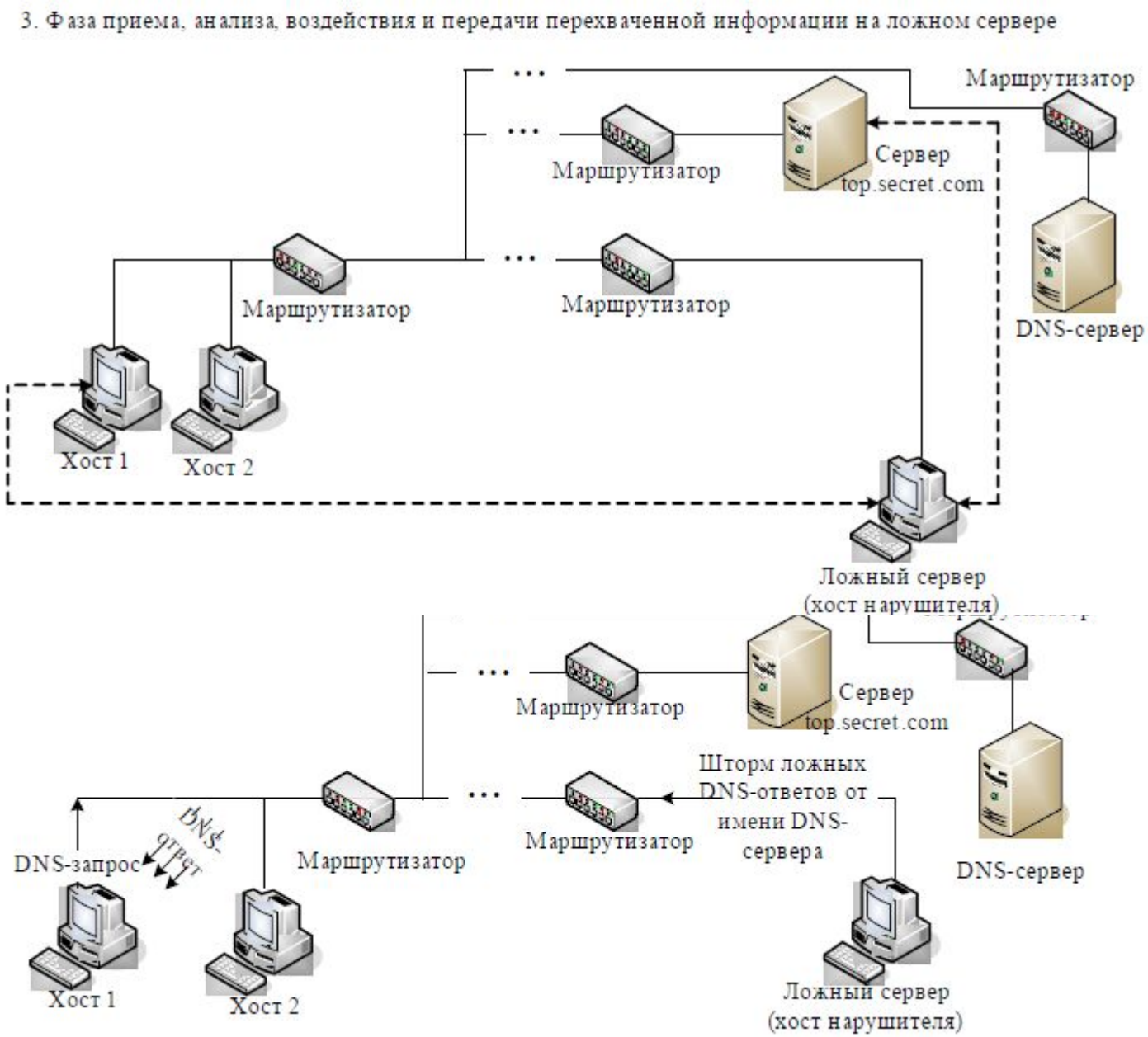


Схема реализации угрозы «Внедрение ложного DNS-сервера» путем шторма DNS-ответов на компьютер сети

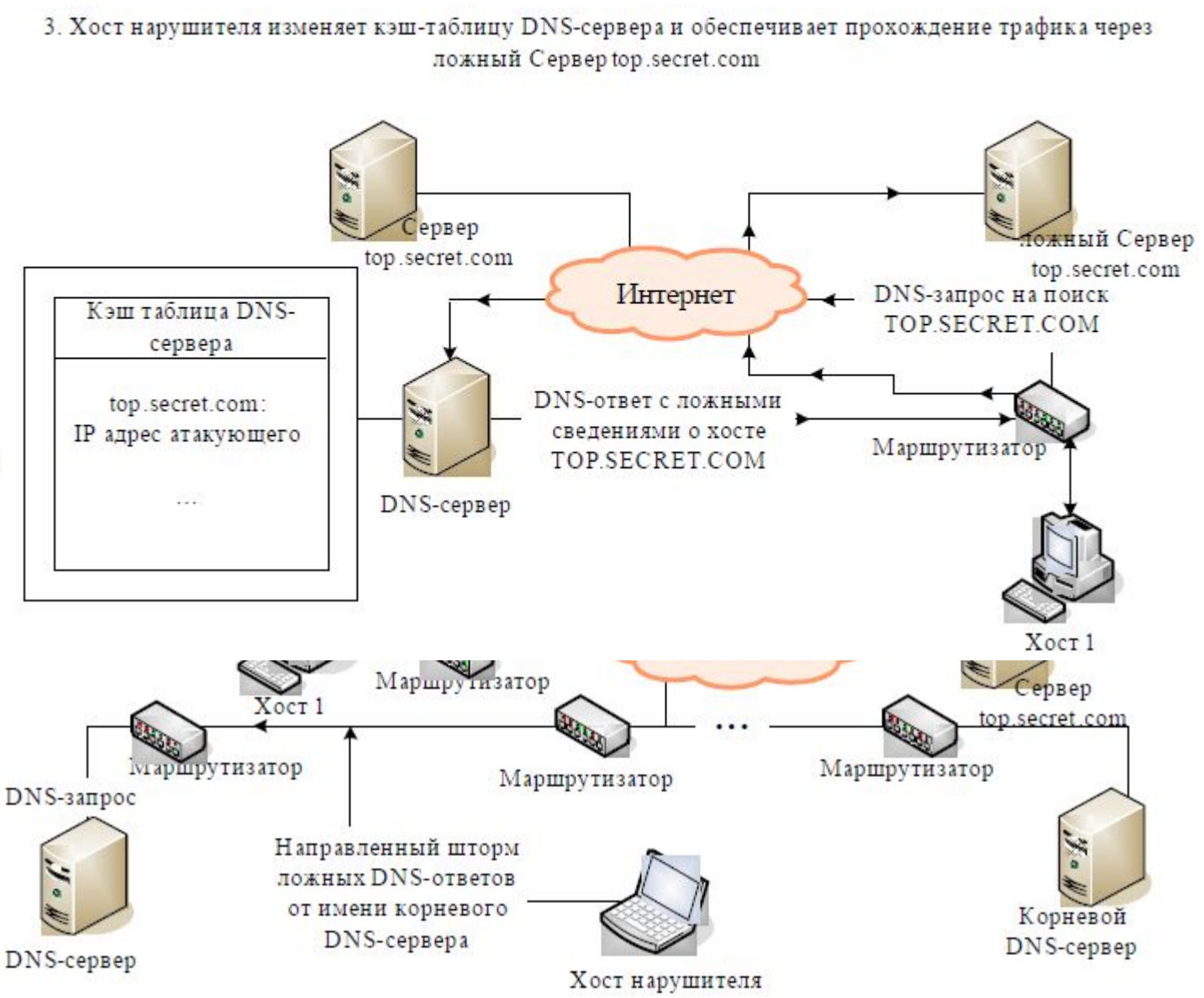
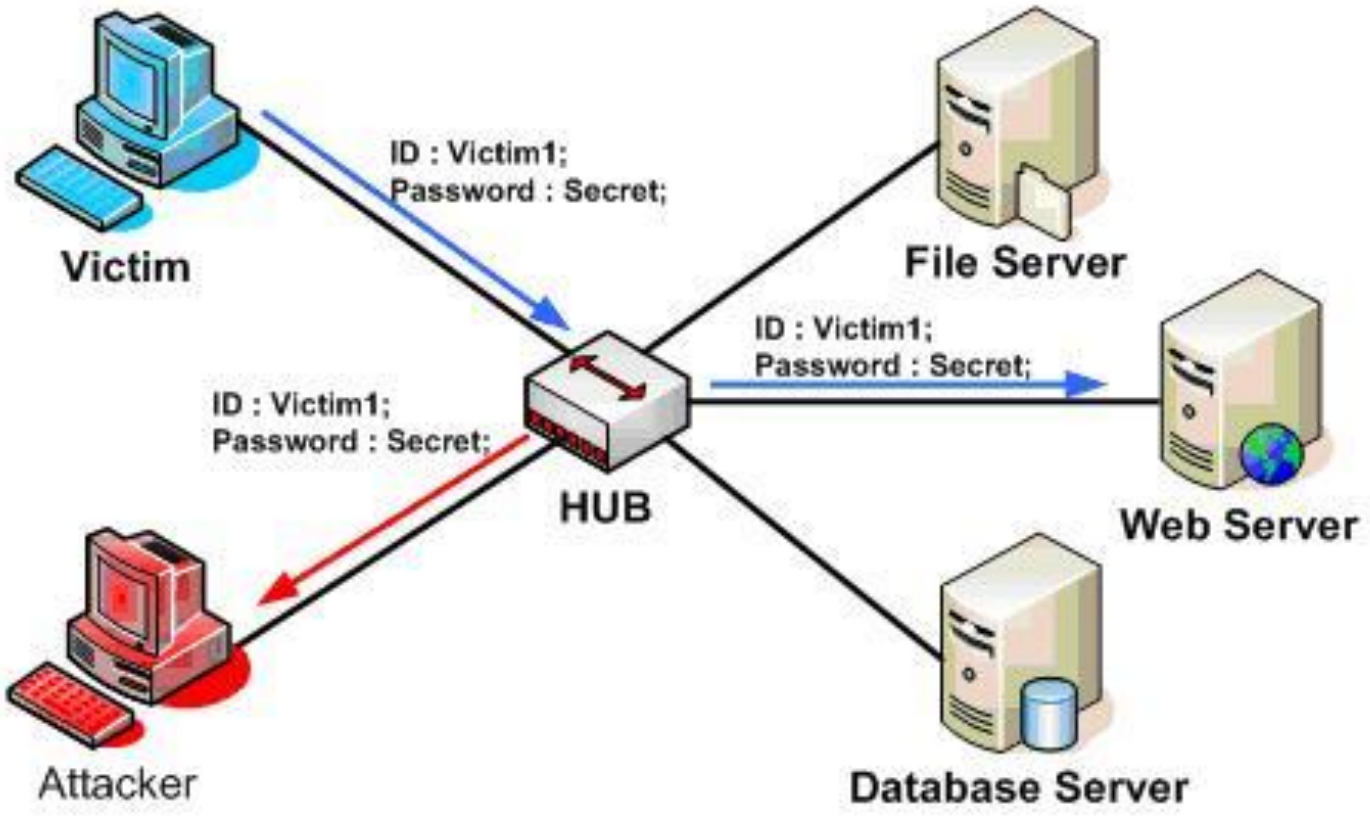


Схема реализации угрозы «Внедрение ложного DNS-сервера» путем шторма DNS-ответов на DNS-сервер

Реализация сетевых атак



Этапы реализации сетевой атаки

1. Сбор информации

- Изучение окружения
- Идентификация топологии атакуемой сети
- Идентификация узлов сети
- Идентификация сервисов или сканирование портов
- Идентификация операционной системы
- Определение роли узла
- Определение уязвимостей узла

Этапы реализации сетевой атаки

2. Реализация атаки

- Проникновение
- Установление контроля
- Цели реализации атаки

3. Завершение атаки

- «Зачистка» журналов регистрации и логов
- Откат сделанных изменений в настройках
- Удаление информации, вспомогательной для атаки

Классификация сетевых атак

- Удаленное проникновение (remote penetration)
- Локальное проникновение (local penetration)
- Удаленный отказ в обслуживании (remote denial of service)
- Локальный отказ в обслуживании (local denial of service)
- Сетевые сканеры (network scanners)
- Сканеры уязвимостей (vulnerability scanners)
- Взломщики паролей (password crackers)
- Анализаторы протоколов (sniffers)

Функции системы обнаружения атак (IDS – Intrusion Detection System)

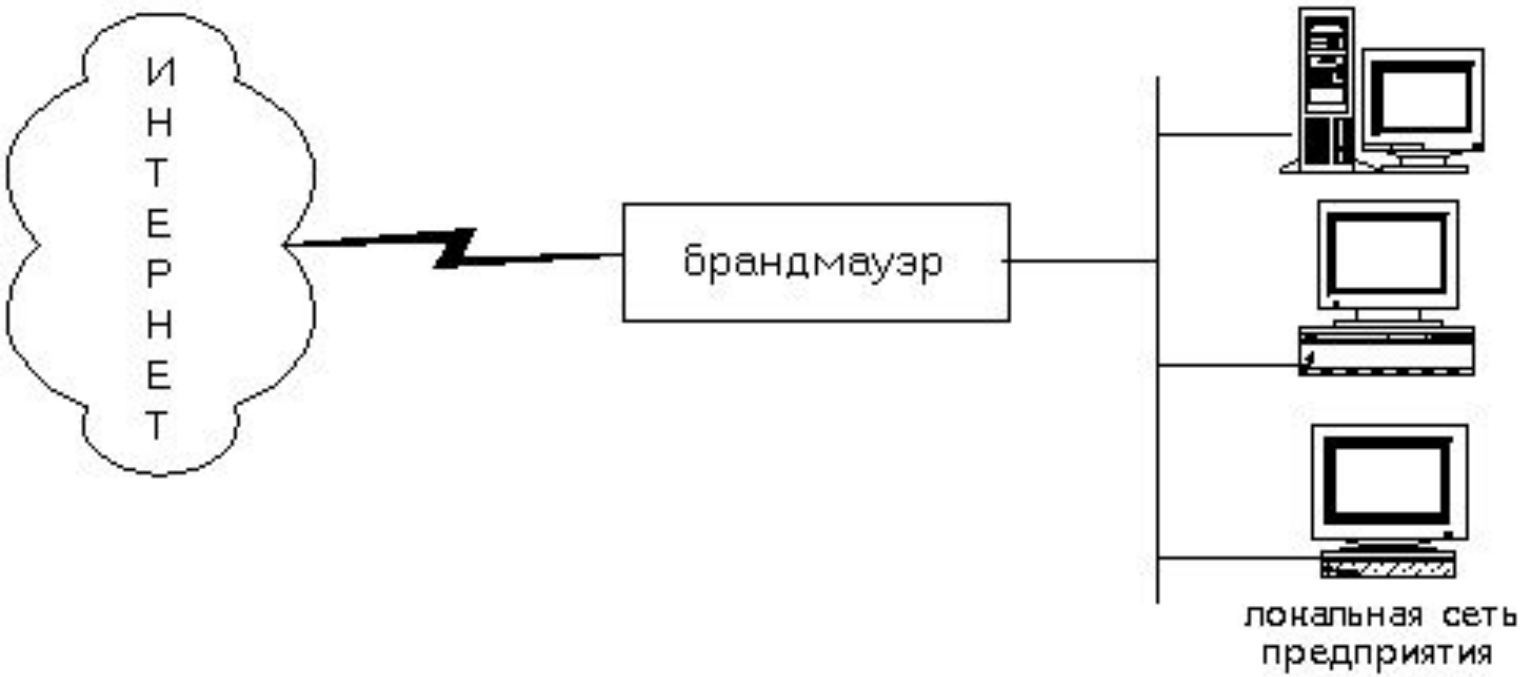
- Распознавание известных атак и предупреждение о них соответствующего персонала
- «Понимание» зачастую непонятных источников информации об атаках
- Освобождение или снижение нагрузки на персонал, отвечающий за безопасность, от текущих рутинных операций
- Возможность управления средствами защиты не-экспертами в области безопасности
- Контроль всех действий субъектов корпоративной сети
- Контроль эффективности межсетевых экранов
- Контроль узлов сети с неустановленными обновлениями или узлов с устаревшим программным обеспечением
- Блокирование и контроль доступа к определенным узлам Internet
- Контроль электронной почты

Варианты реагирования IDS на обнаруженную сетевую атаку

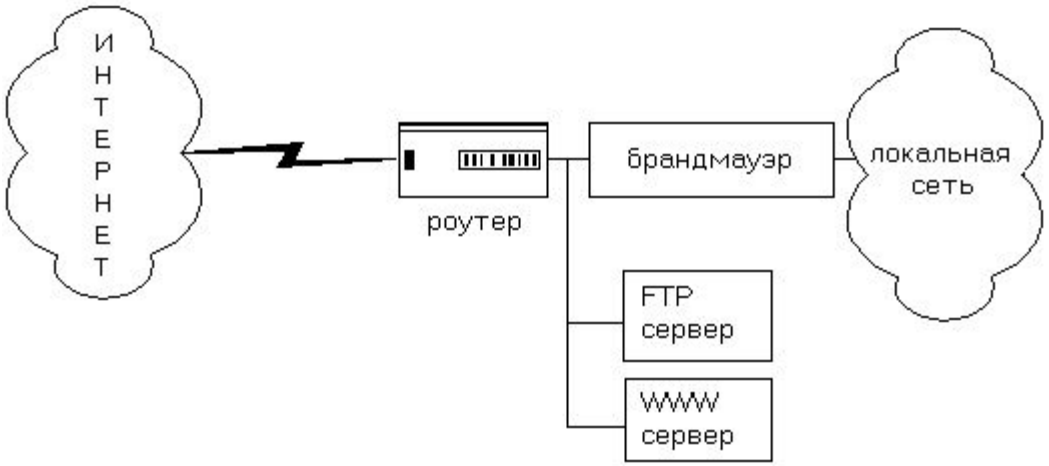
- Уведомление на консоль системы обнаружения атак или на консоль интегрированной системы
- Звуковое оповещение об атаке
- Генерация управляющих последовательностей SNMP для систем сетевого управления
- Генерация сообщения об атаке по электронной почте
- Дополнительные уведомления на пейджер или факс
- Обязательная регистрация обнаруживаемых событий
- Трассировка событий
- Прерывание действий атакующего, т.е. завершение соединения
- Реконфигурация сетевого оборудования или межсетевых экранов
- Блокирование сетевого трафика

Сетевая безопасность

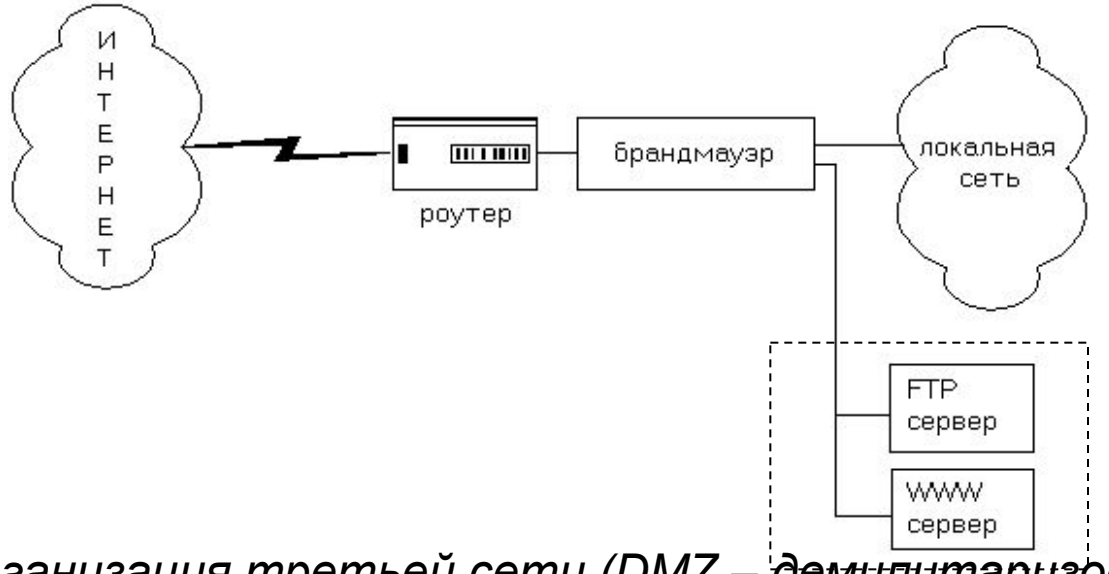
Межсетевой экран или брандмауэр (по-нем. *brandmauer*, по-англ. *firewall*, по-рус. о*гненная стена*) это система или комбинация систем, позволяющих разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую



Сетевая безопасность



Защита только одной подсети



Организация третьей сети (DMZ – демилитаризованной зоны)

Пакетные фильтры. Брандмауэры с пакетными фильтрами принимают решение о том, пропускать пакет или отбросить, просматривая IP-адреса, флаги или номера TCP портов в заголовке этого пакета.

Для описания правил прохождения пакетов составляются таблицы типа:

Действие	тип пакета	адрес источника	порт источника	адрес назначения	порт назначения	флаги

Достоинства пакетных фильтров:

+ относительно невысокая стоимость;
+ гибкость в определении правил фильтрации;
+ небольшая задержка при прохождении пакетов.

Недостатки пакетных фильтров:

- локальная сеть видна (маршрутизируется) из Internet;
- правила фильтрации пакетов трудны в описании, требуются очень хорошие знания технологий TCP и UDP;
- при нарушении работоспособности брандмауэра все компьютеры за ним становятся полностью незащищенными либо недоступными;
- аутентификацию с использованием IP-адреса можно обмануть использованием IP-спуфинга (атакующая система выдает себя за другую, используя ее IP-адрес);
- отсутствует аутентификация на пользовательском уровне.

Достоинства серверов прикладного уровня:

+ локальная сеть невидима из Internet;
+ при нарушении работоспособности брандмауэра пакеты перестают проходить через брандмауэр, тем самым не возникает угрозы для защищаемых им машин;
+ защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, снижая тем самым вероятность взлома с использованием дыр в программном обеспечении;
+ аутентификация на пользовательском уровне может быть реализована как система немедленного предупреждения о попытке взлома.

Недостатки серверов прикладного уровня:

- более высокая, чем для пакетных фильтров стоимость;
- невозможность использовании протоколов RPC и UDP;
- производительность ниже, чем для пакетных фильтров.

Атаки на среду передачи информации
Атаки на узлы коммутации сетей

Атаки на среду передачи информации

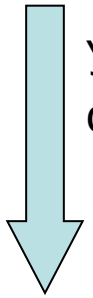
Основной вид атаки на среду передачи - **прослушивание**

В отношении прослушивания все линии связи делятся на:

* широковещательные с неограниченным доступом
* широковещательные с ограниченным доступом
* соединение «точка-точка»

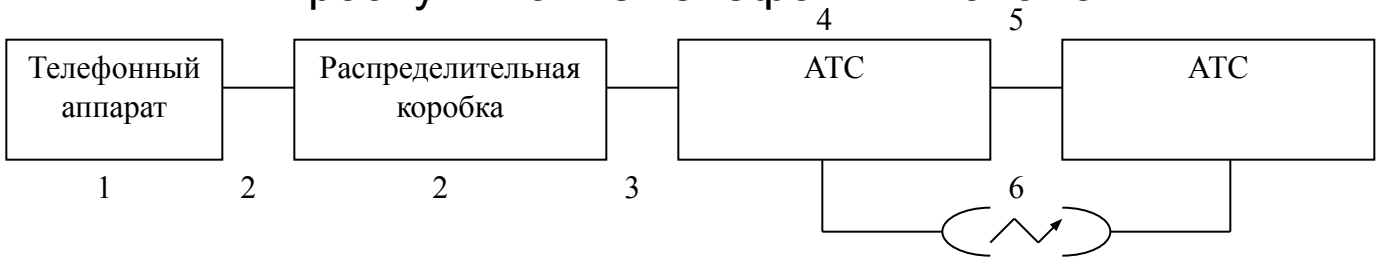
Возможность прослушивания кабельных соединений:

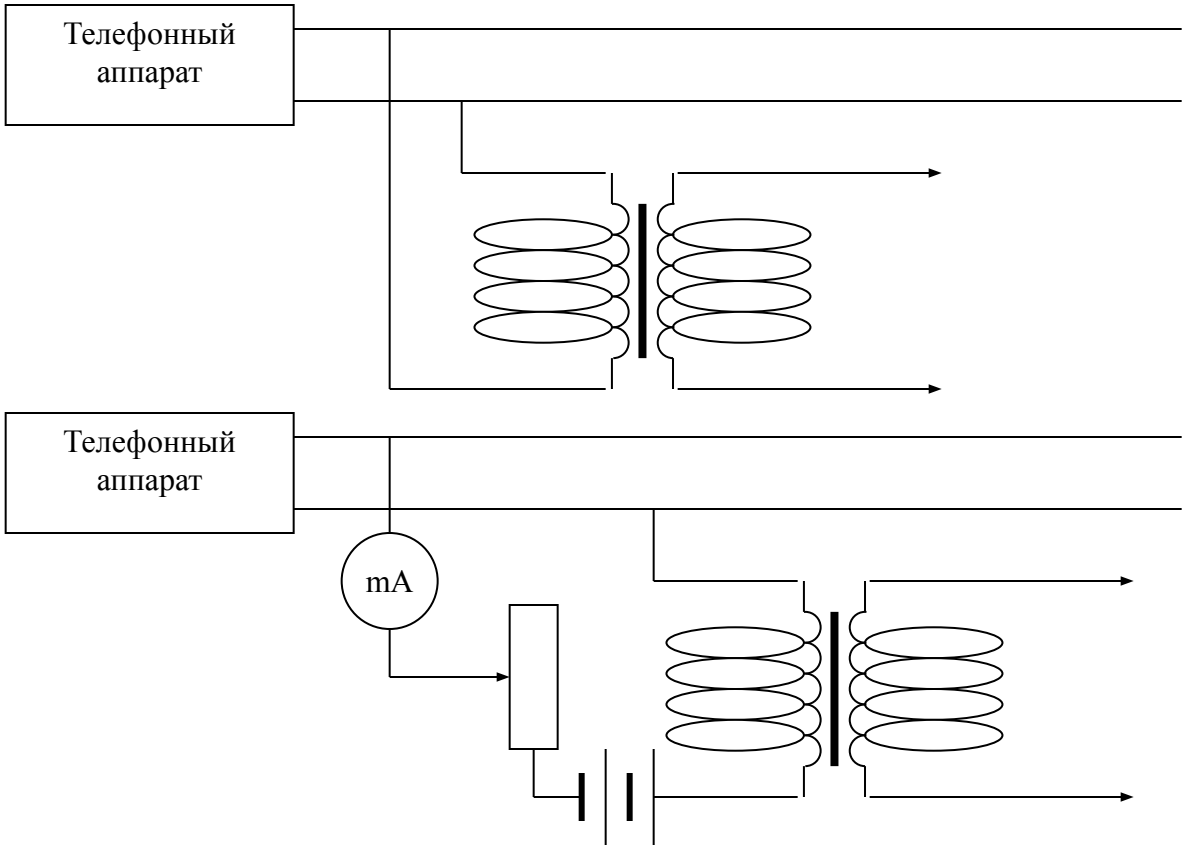
* невитая пара
* витая пара
* коаксиальный кабель
* оптоволоконный кабель

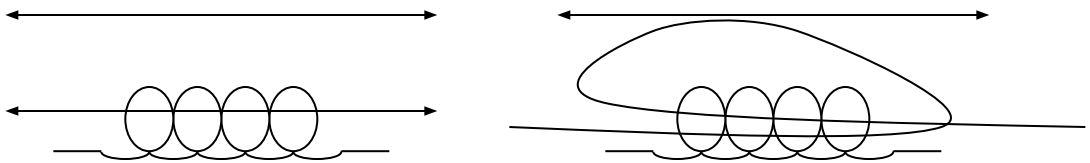


Увеличение сложности

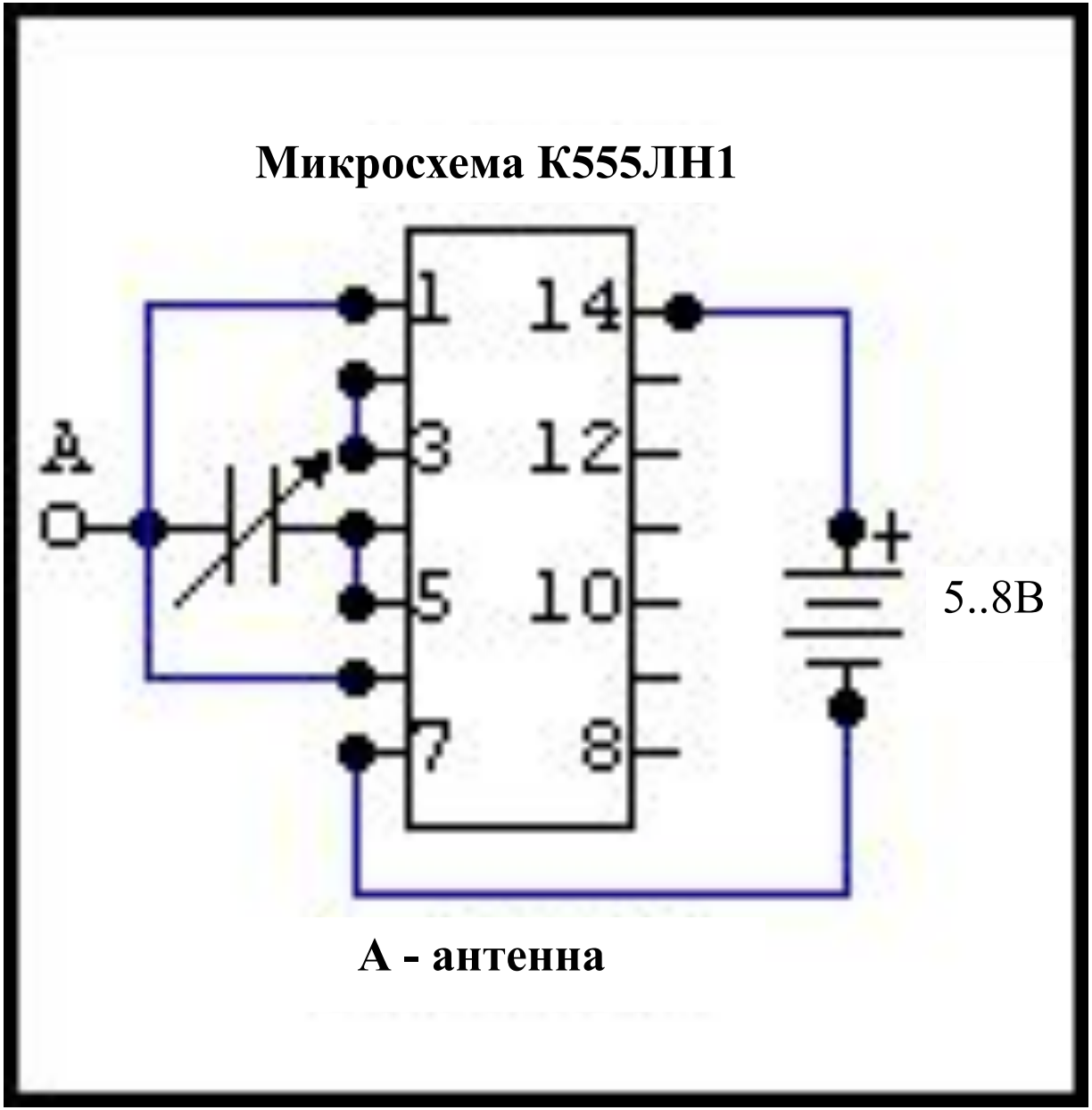
Прослушивание телефонных каналов



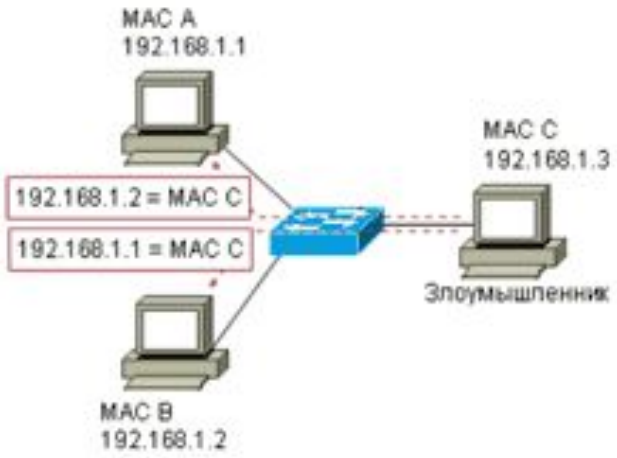


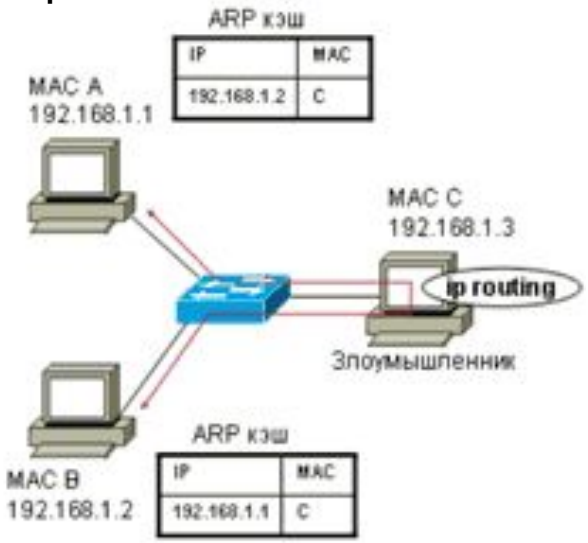


Глушение радиоканала



Атаки на коммутатор Ethernet

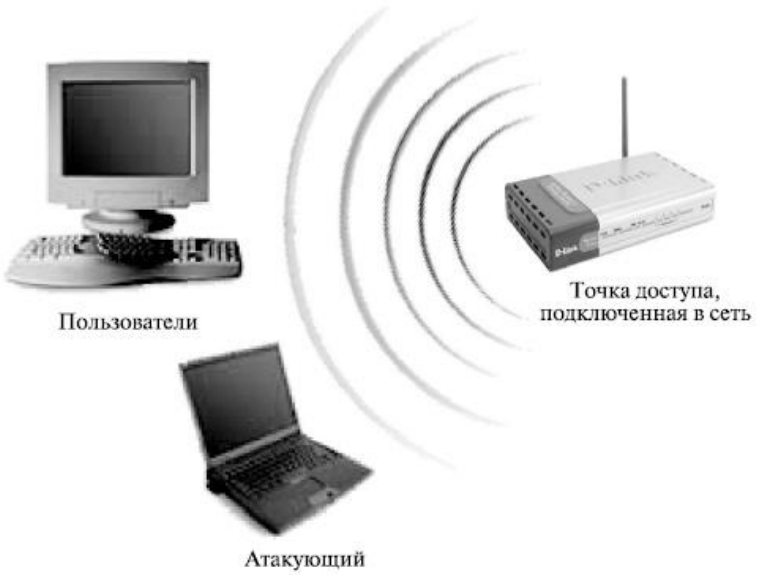


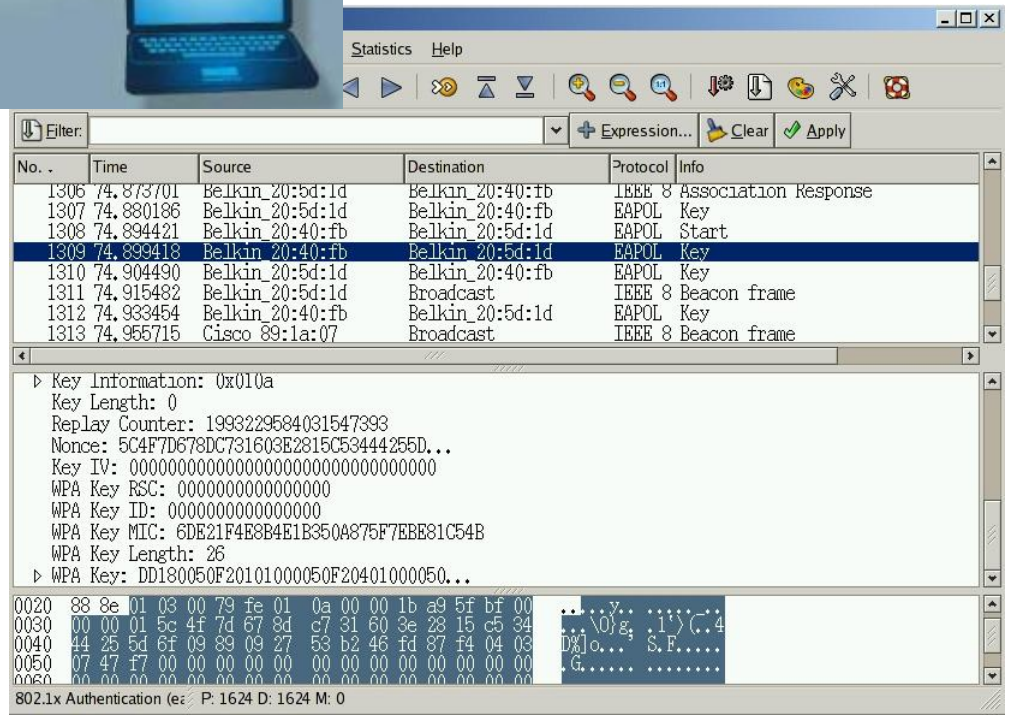


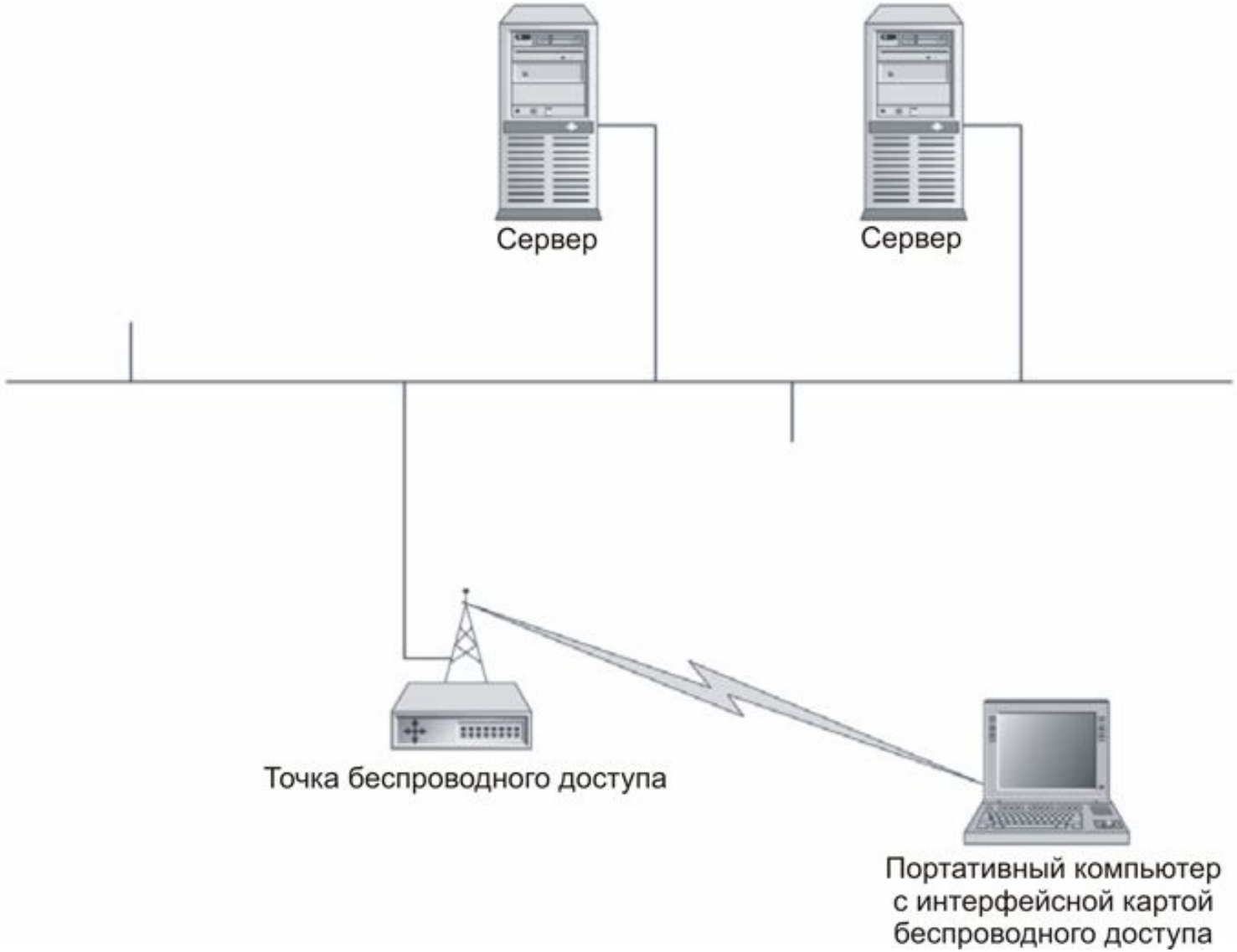
Посылка ARP сообщений атакуемым компьютерам

Перехват трафика или атака типа «man in the middle»

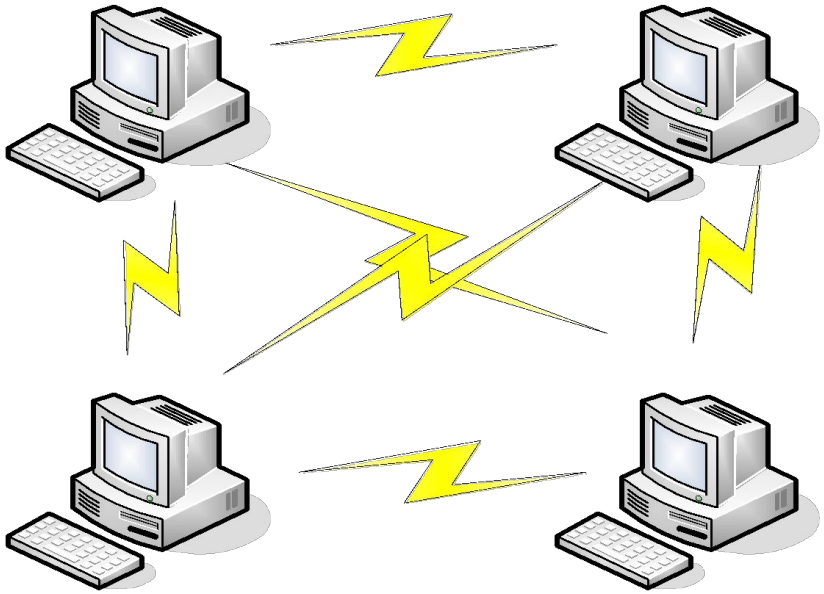
Атаки на беспроводные сети



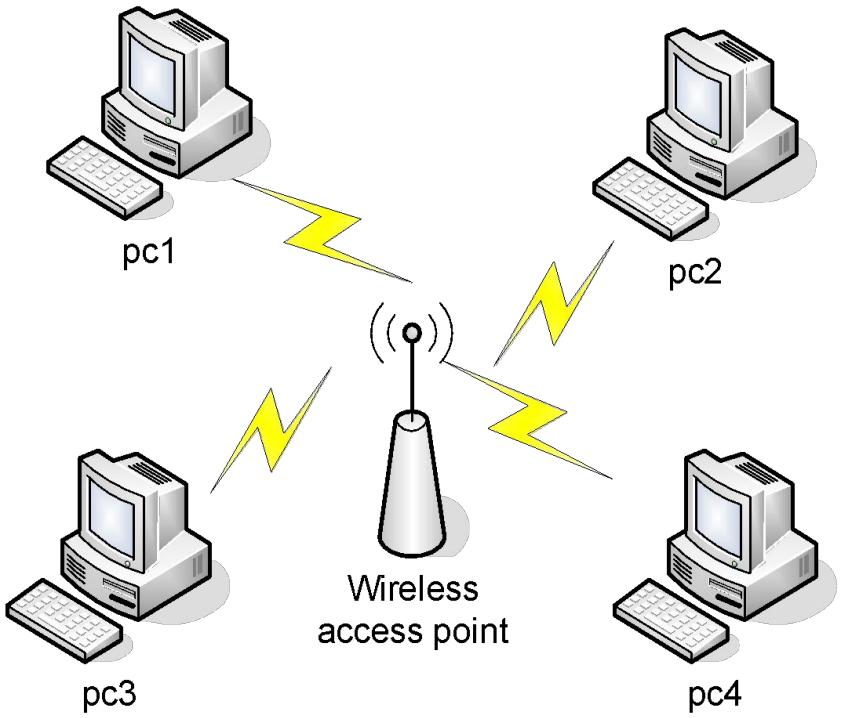




Типичная организация беспроводной сети



Режим работы Ad Hoc



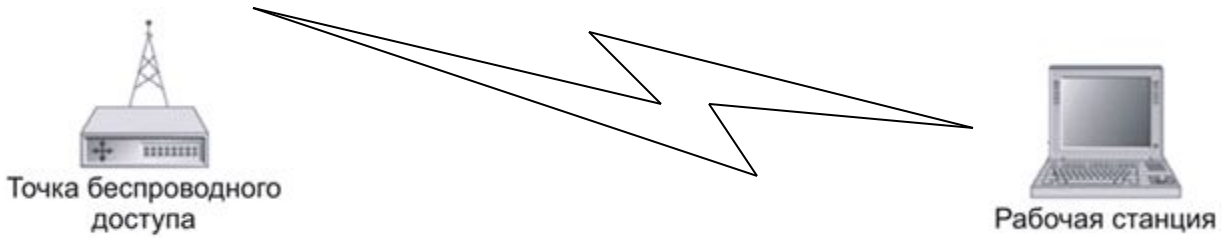
Режим работы Infrastructure Mode

1. Рабочая станция передает запрос на аутентификацию точке доступа

2. Точка доступа передает случайный вызов рабочей станции

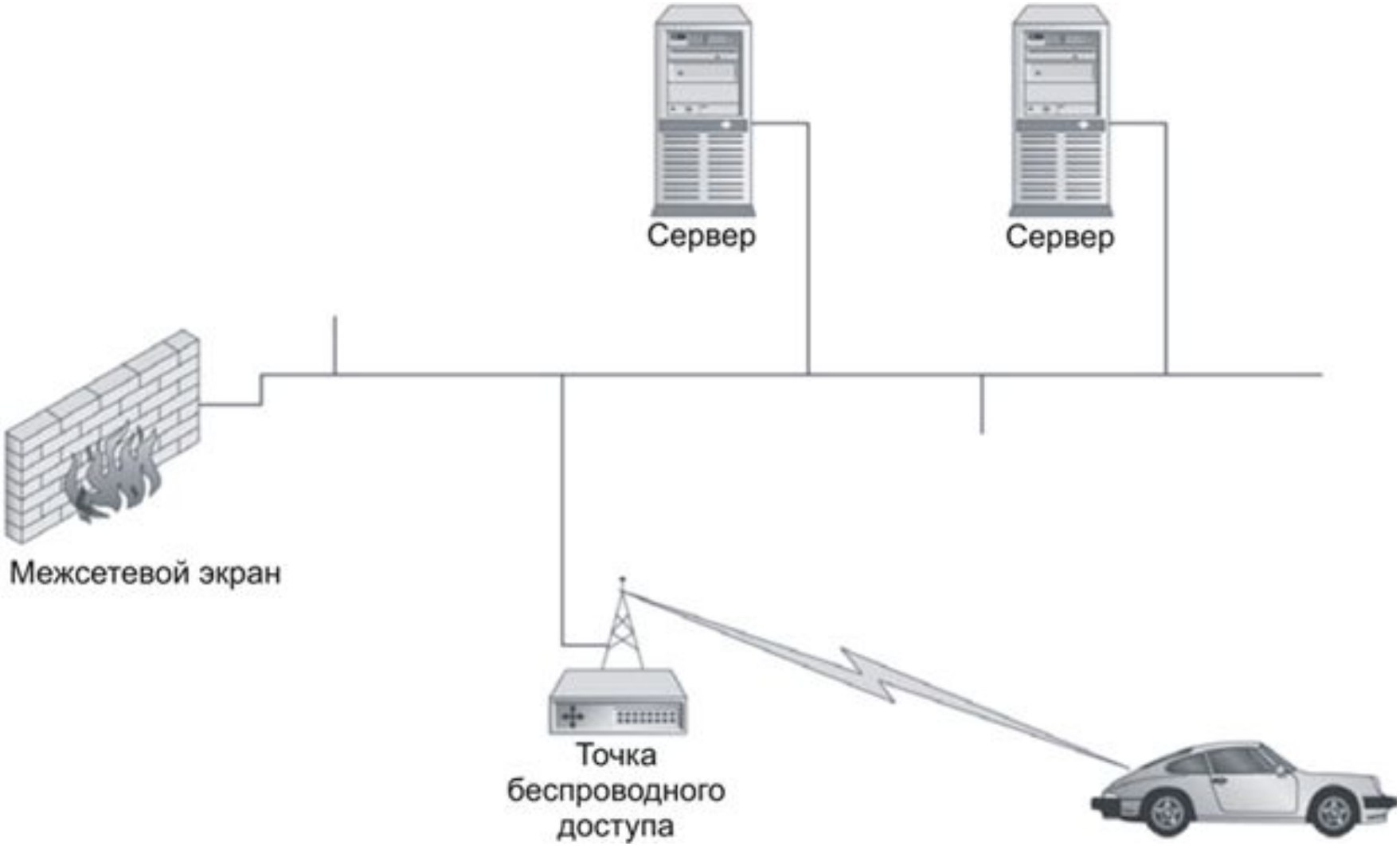
3. Рабочая станция отправляет на точку доступа ответ, зашифрованный с использованием общего секрета

4. Если вызов правильно расшифровывается, точка доступа подтверждает успешную аутентификацию

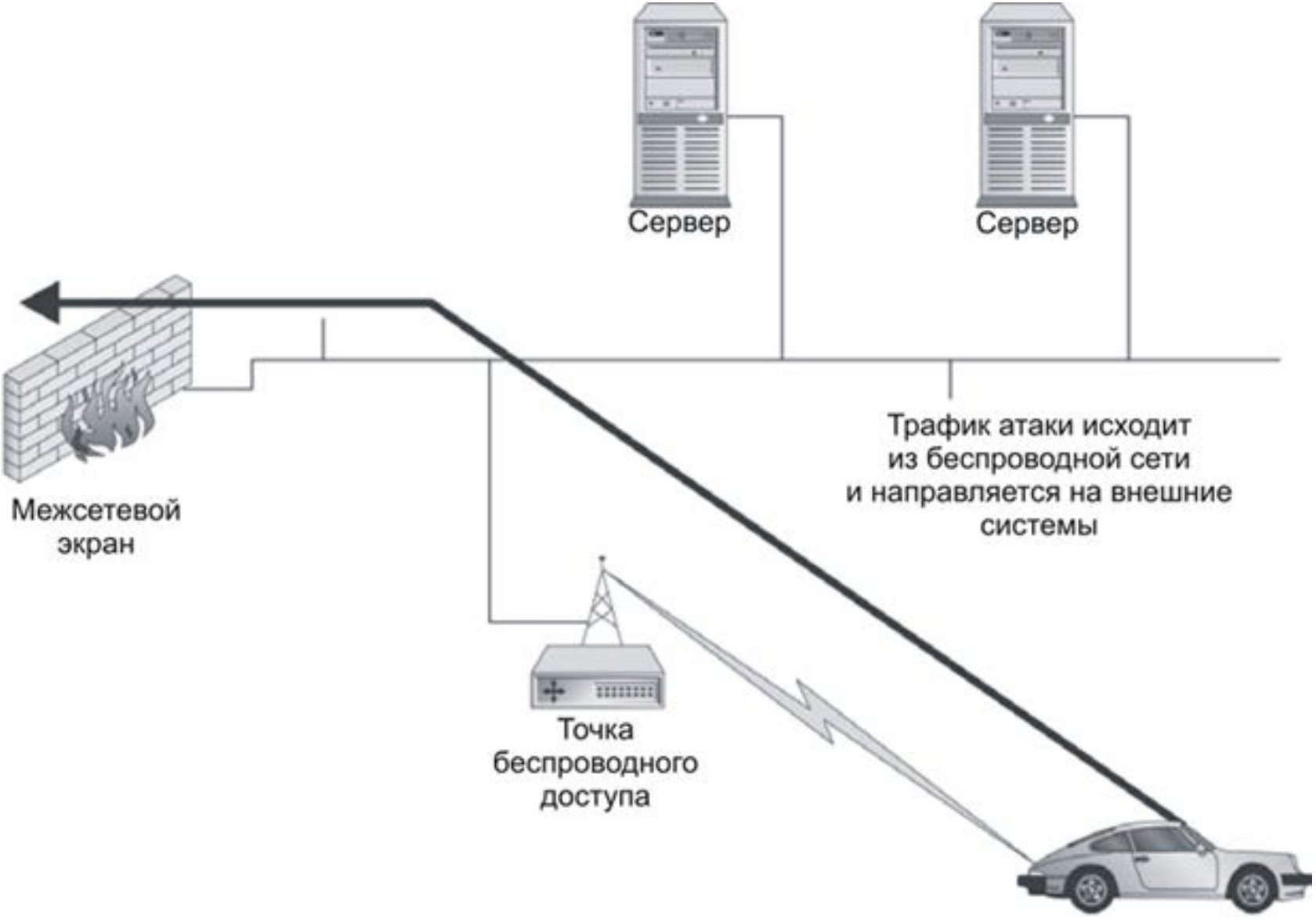


Аутентификационный обмен WEP

Атака на WEP через посредника (man-in-the-middle)



Прослушивание сети WLAN



Атака на внешние системы

Основные положения политики безопасности беспроводных сетей

· Уменьшить зону радиопокрытия (до минимально приемлемой). В идеальном варианте, зона радиопокрытия сети не должна выходить за пределы контролируемой территории.

· Изменить пароль администратора, установленный по умолчанию

· Активизировать фильтрацию по MAC-адресам

· Запретить широковещательную рассылку идентификатора сети (SSID)

· Изменить идентификатор сети (SSID), установленный по умолчанию

· Периодически изменять идентификатор сети (SSID)

Основные положения политики безопасности беспроводных сетей

- Активизировать функции WPA2
- Периодически изменять WPA2-ключи
- Установить и настроить персональные МЭ и антивирусные программы у абонентов беспроводной сети
- Выполнить соответствующие настройки фильтрации трафика на телекоммуникационном оборудовании и межсетевых экранах
- Обеспечить резервирование оборудования, входящего в состав беспроводной сети
- Обеспечить резервное копирование ПО и конфигураций оборудования
- Осуществлять периодический мониторинг состояния защищенности беспроводной сети с помощью специализированных средств анализа защищенности для беспроводных сетей.

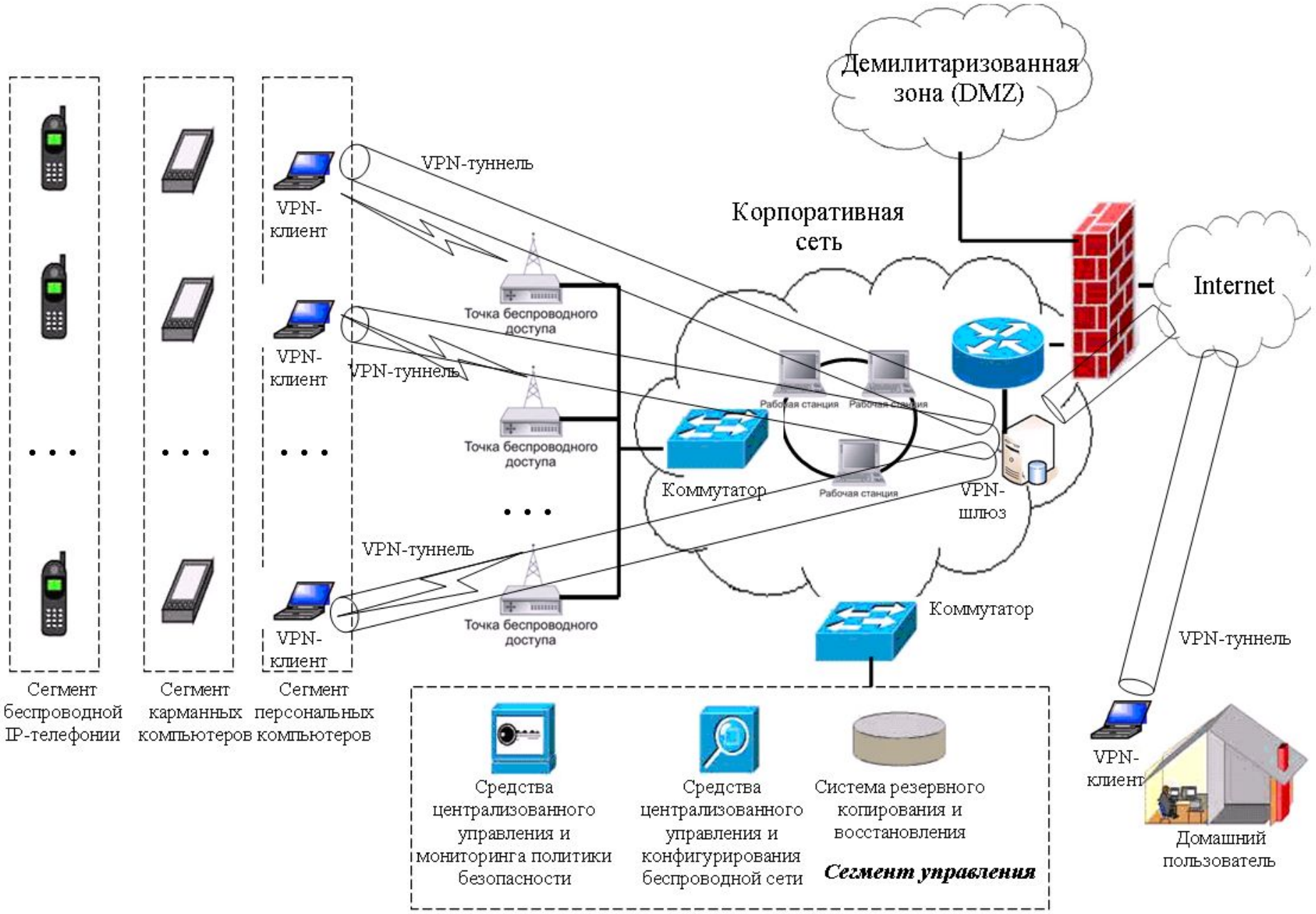


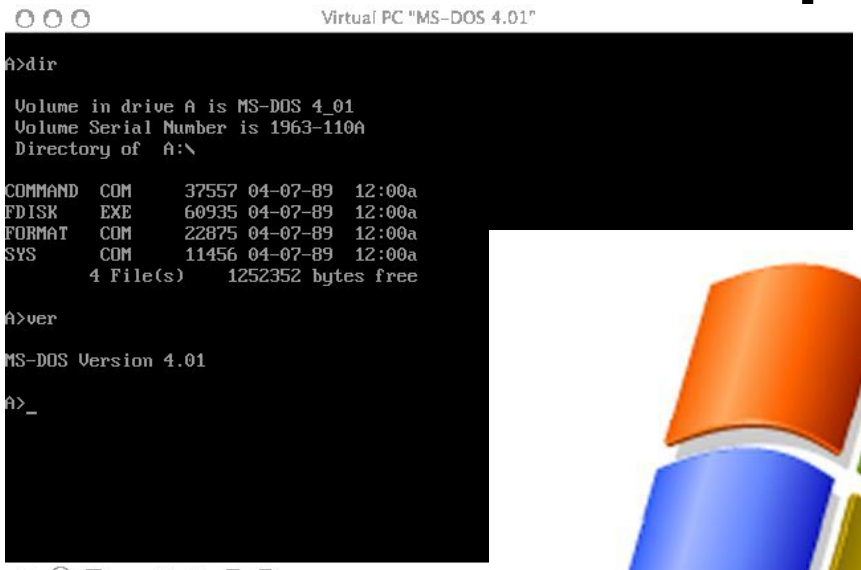
Схема защищенного беспроводного сегмента корпоративной сети

Защита мобильных устройств связи

Защита мобильных устройств

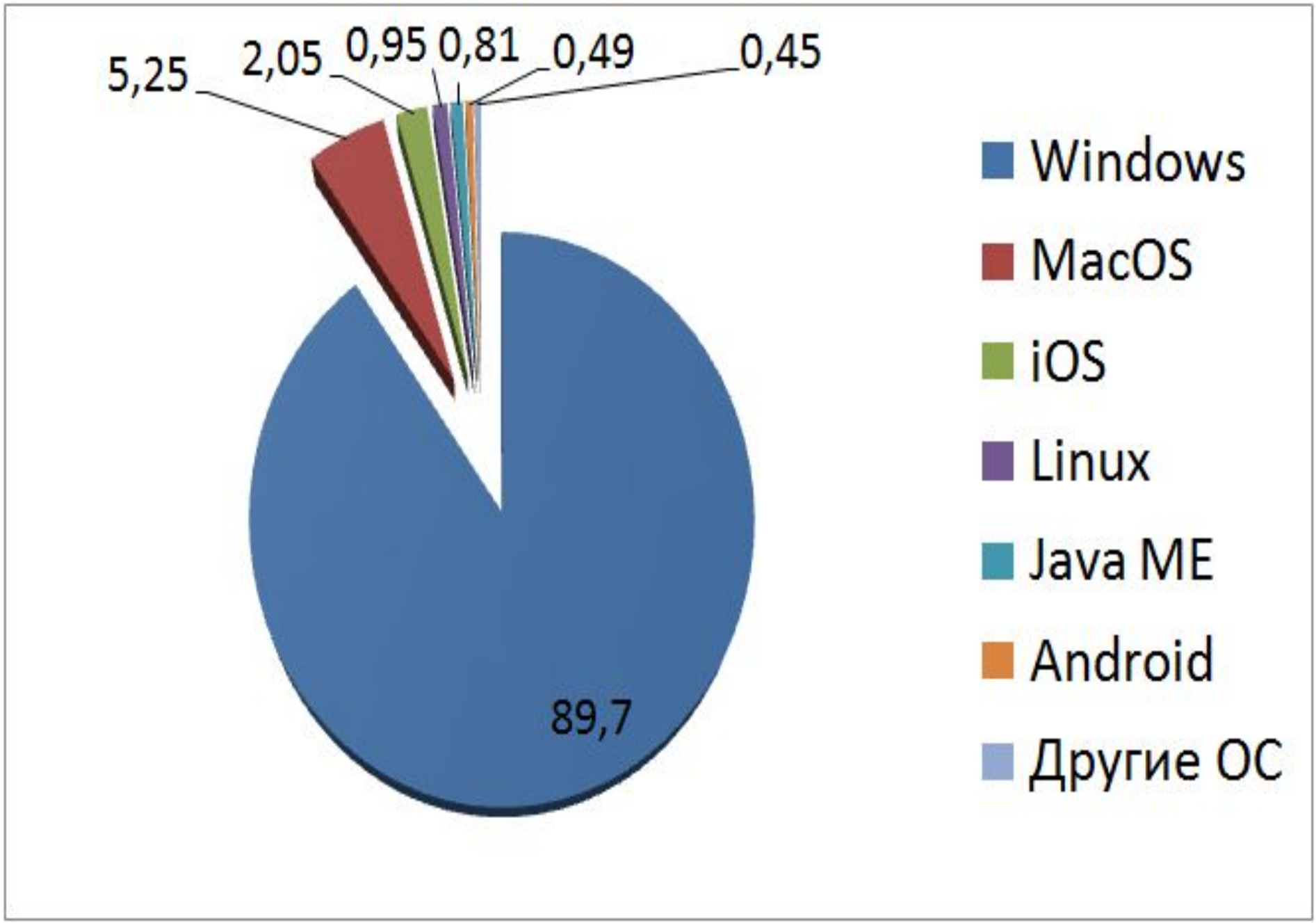
1. Постоянно растет процент КПК и смартфонов среди используемых для мобильной связи устройств. Чем популярнее технология, тем проще и выгоднее ее атаковать
2. По мере того, как область расширяется, увеличивается и количество квалифицированных специалистов, потенциально способных атаковать ее безопасность
3. КПК и смартфоны становятся все более мощными и функциональными. Это значит, что у вирусов и вирусописателей появляется все больше возможностей
4. Увеличение функциональности устройства естественным образом ведет к увеличению количества потенциально интересной информации, которая в нем хранится

Безопасность операционных систем



«Операционная система не должна заменять владельцу компьютера руки и голову» (Народная мудрость)

Рыночная доля операционных систем в мире на начало 2011 года



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 17 декабря 2010 г. № 2299-р

МОСКВА

1. Утвердить прилагаемый план перехода федеральных органов исполнительной власти и федеральных бюджетных учреждений на использование свободного программного обеспечения на 2011 - 2015 годы.

2. Федеральным органам исполнительной власти обеспечить выполнение мероприятий в соответствии с планом, утвержденным настоящим распоряжением, в пределах установленной Правительством Российской Федерации предельной численности их работников и бюджетных ассигнований, предусмотренных им в федеральном бюджете на выполнение полномочий в установленной сфере деятельности.

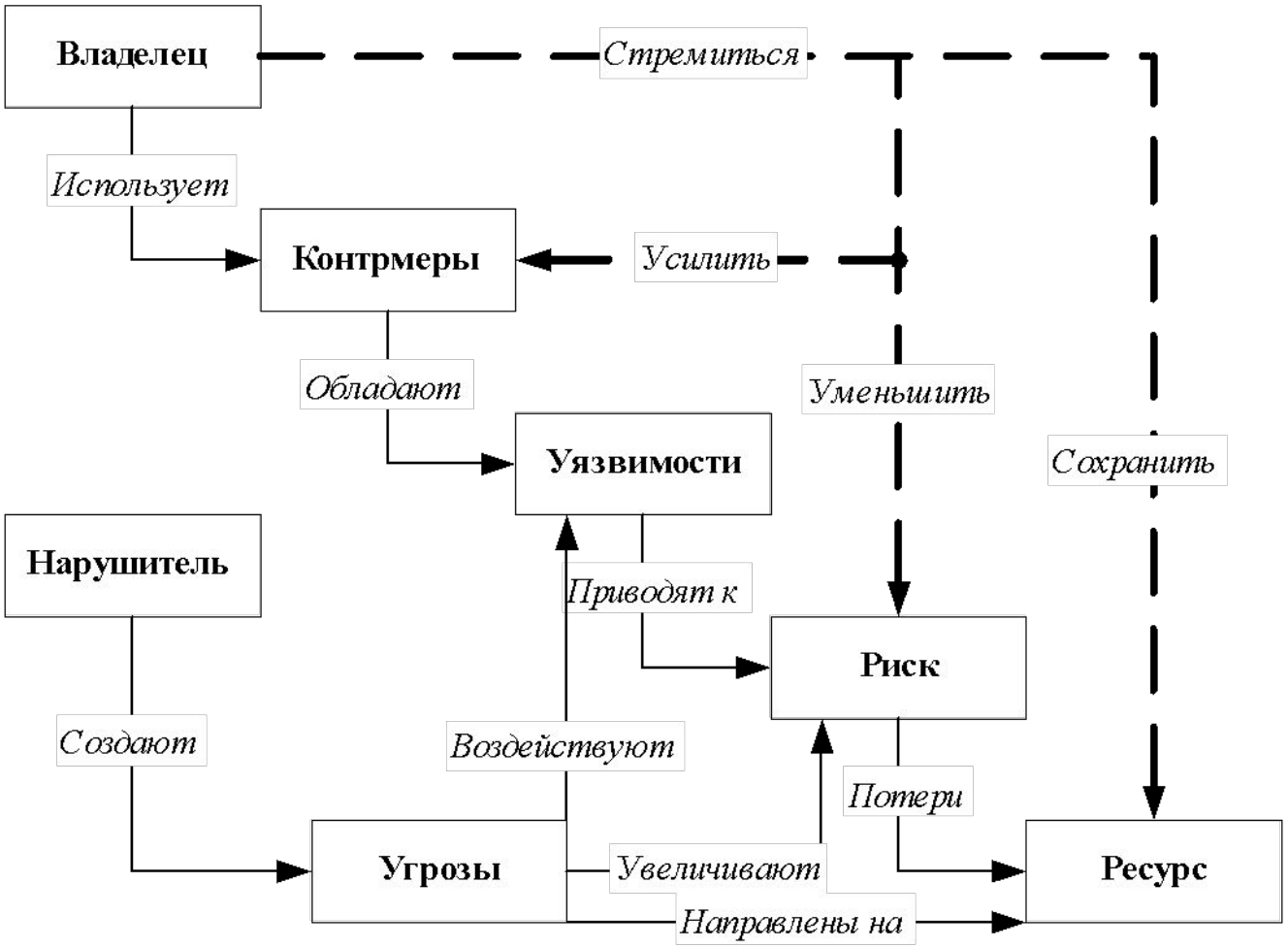
Председатель Правительства
Российской Федерации В.Путин

Основные проблемы безопасности операционных систем

1. Нет обновления компонентов системы
2. Права администратора там, где не нужно
3. Умышленное отключение встроенных механизмов безопасности (например, UAC в Windows 7)
4. Пустые или примитивные пароли
5. Некорректное удаление программ

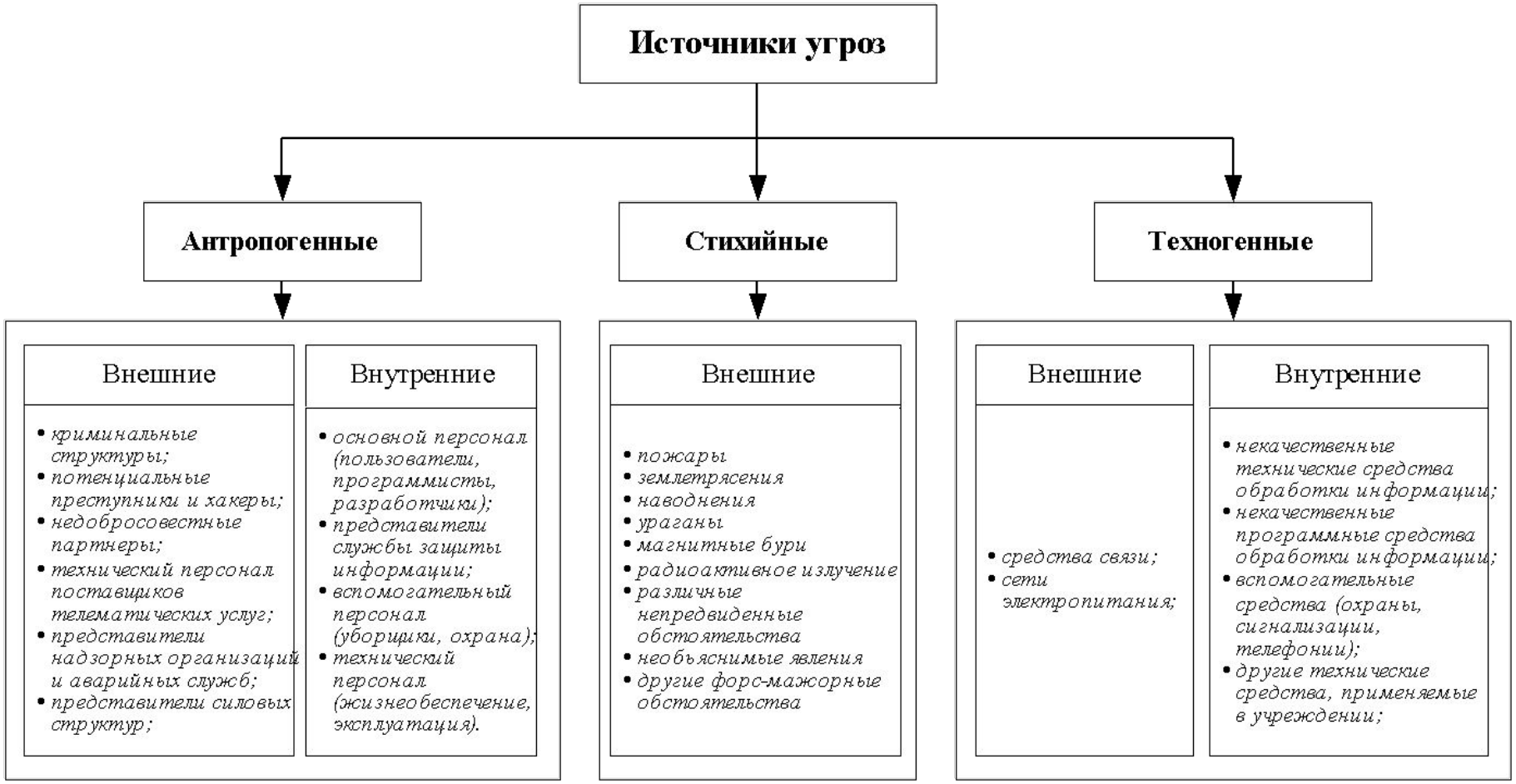
Раздел четвертый

«Защита информационных ресурсов предприятия»

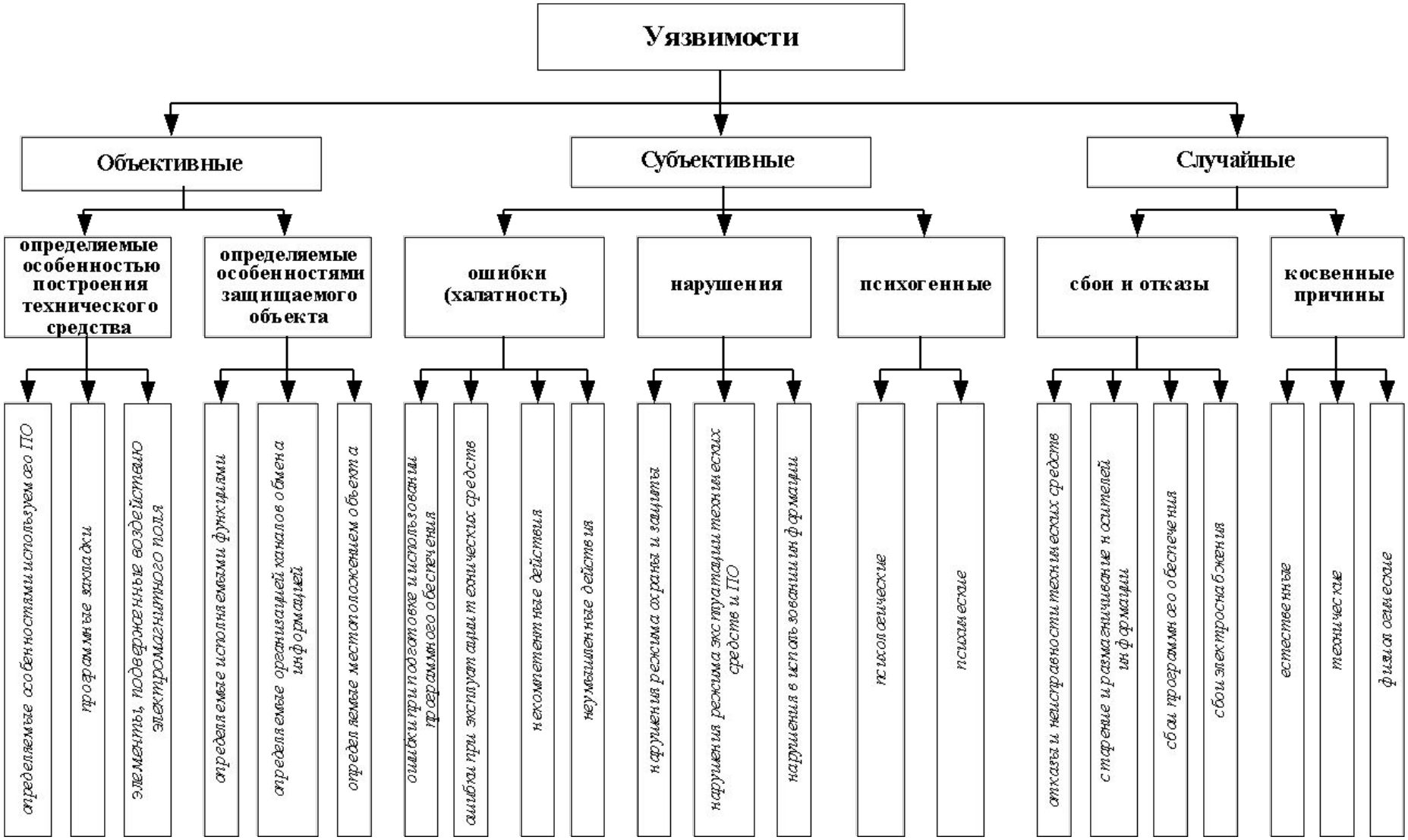


Модель построения системы защиты информации

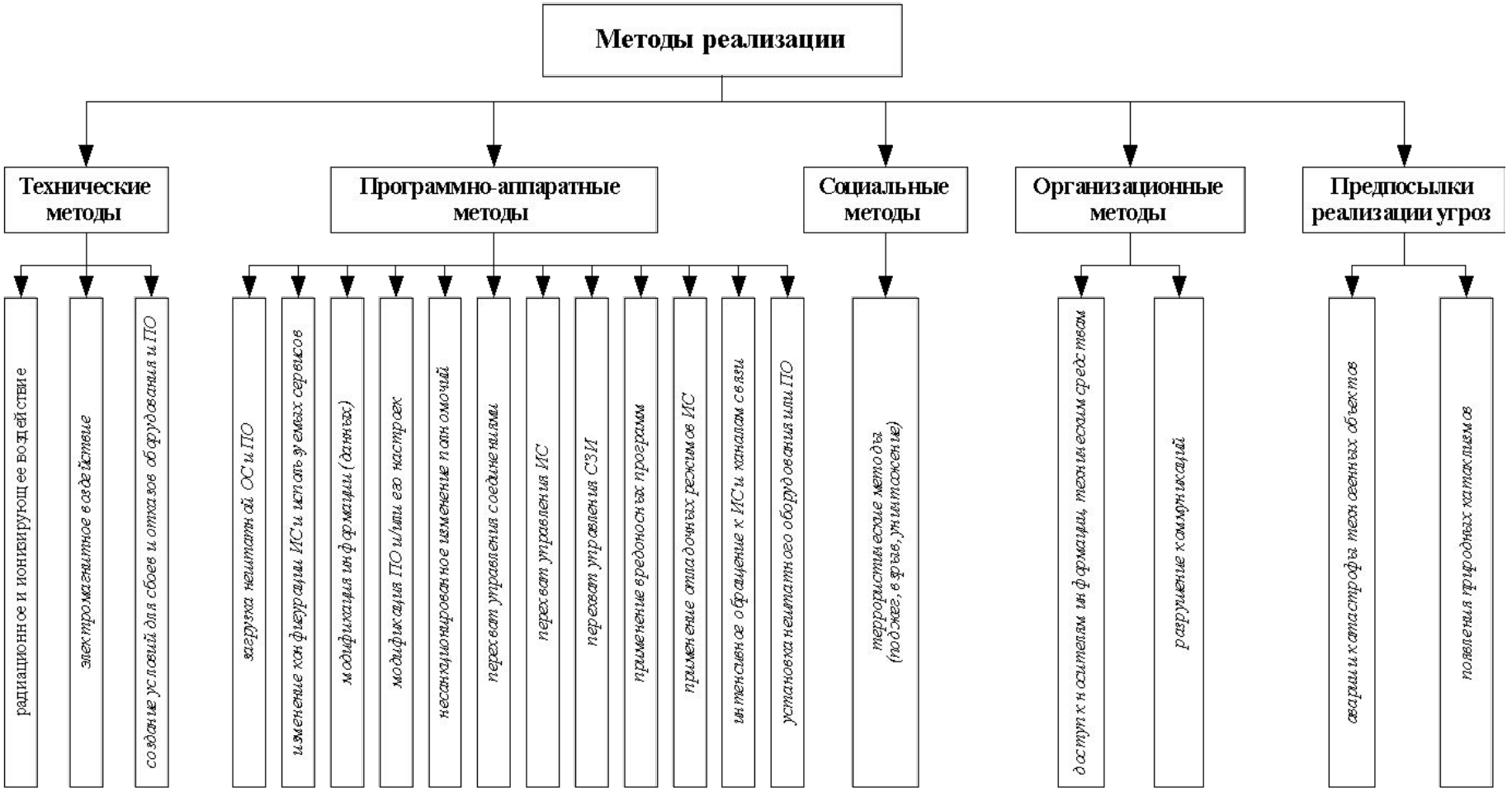
Модель реализации угроз информационной безопасности



Классификация по типу источника угрозы



Классификация уязвимостей



Классификация методов реализации

Комплексная система безопасности

События, предшествующие появлению инсайдера

Конфликт	20%
Увольнение	47%
Отсутствие повышения	13%
Другие	20%

Портрет типичного инсайдера

Инженер	14%
Программист	21%
Системный администратор	38%
Специалист по IT	14%
Другое	13%

Самые опасные угрозы информационной безопасности

Нарушение конфиденциальности информации	85%
Искажение информации	64%
Мошенничество	49%
Саботаж	41%
Утрата информации	25%
Сбои в работе ИС	18%
Кража оборудования	11%

Негативные последствия утечки информации

Удар по репутации и плохое паблисити	51%
Потеря клиентов	43%
Прямые финансовые убытки	36%
Снижение конкурентоспособности	29%
Преследование надзорными/правоохранительными органами	21%
Потеря партнеров	18%
Судебное преследование и юридические издержки	2%

Каналы утечки информации

Мобильные накопители	85%
Электронная почта	83%
Интернет (веб-почта форумы)	81%
Интернет пейджеры	77%
Печатающие устройства	65%
Фотопринадлежности	30%

Используемые средства информационной безопасности

Антивирусное ПО	100%
Межсетевые экраны	79%
Контроль доступа	68%
Антиспамовое ПО	44%
IDS/IPS	26%
VPN	17%
Защита от утечки данных	8%

Препятствия на пути внедрения защиты от утечки информации

Бюджетные ограничения	22%
Психологические препятствия	18%
Юридические препятствия	9%
Отсутствие технологических решений	3%
Отсутствие стандартов	30%
Нехватка квалифицированного персонала	15%

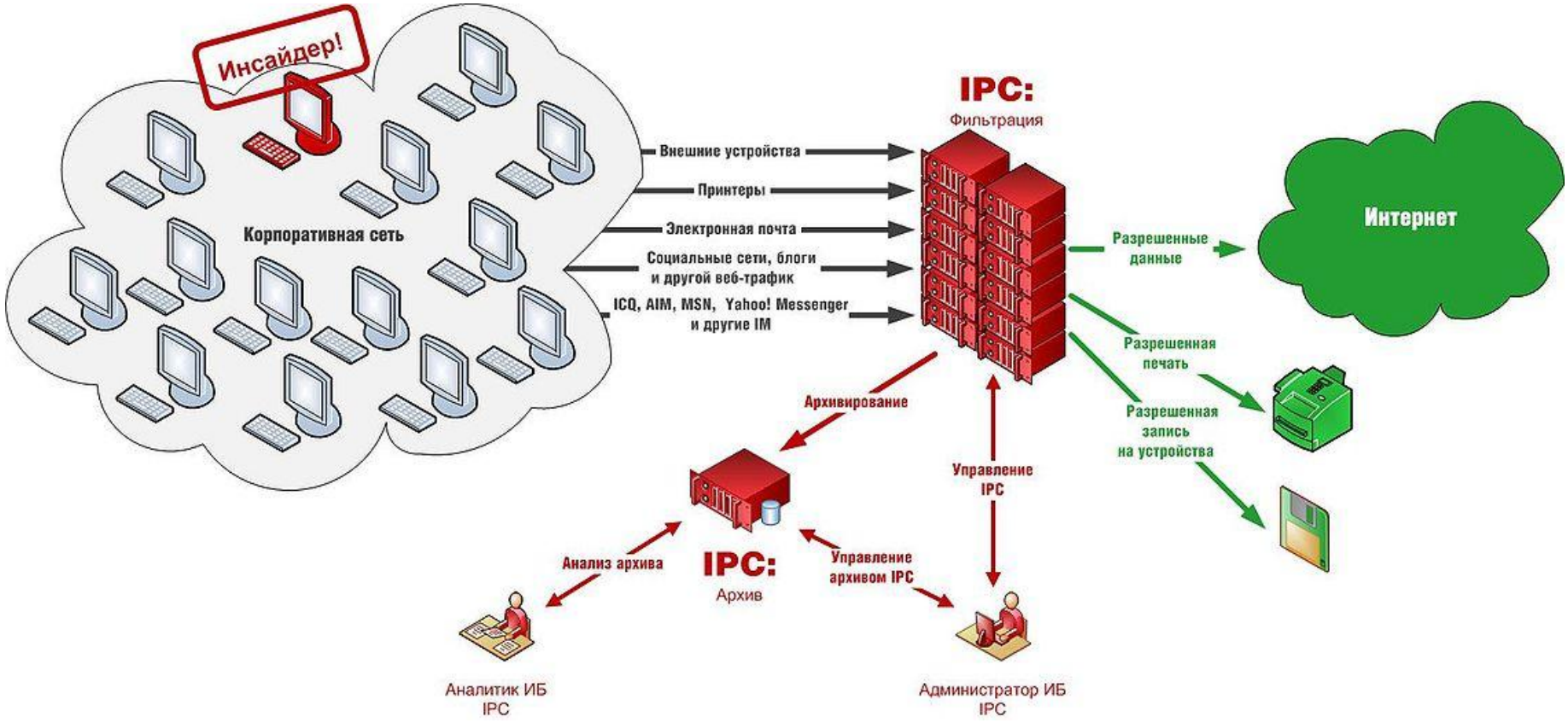
Наиболее эффективные пути защиты от утечки информации

Организационные меры	27%
Внедрение комплексных решений на основе ИТ	49%
Ограничение с внешними сетями	11%
Тренинги сотрудников	9%
Другие	4%

Российские компании несут тяжелые потери от инсайдеров

Information Protection and Control (IPC) — технология защиты конфиденциальной информации от внутренних угроз

Контроль каналов утечки информации (Data Loss Prevention, DLP)



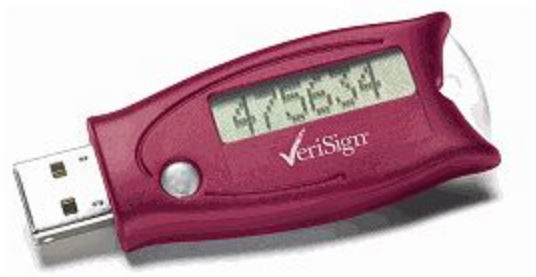
Российские компании несут тяжелые потери от инсайдеров

1. USB-токен легко помещается на цепочке с ключами и позволяет обойтись без считывателей. Пользователю достаточно подсоединить токен, ввести PIN-код, и он сразу получает доступ к сетевым ресурсам.

2. Они позволяют следить за активностью пользователя на протяжении всего сеанса работы, а не только на этапе аутентификации.

3. Возможность использования различных кодов позволяет администраторам более гибко управлять доступом к файлам и приложениям.

4. Многие устройства используют одновременно закрытые ключи и сертификаты, обеспечивая, таким образом, основу для двухфакторной аутентификации. Одно устройство открывает доступ к локальной сети, Интернет, VPN-сети – пользователю достаточно иметь лиш[illegible] и PIN-ко[illegible]



Методы поиска и борьбы с инсайдерами

1. Сигнатурный метод
2. «Цифровые отпечатки» (Digital Fingerprints)
3. Метод расстановки меток
4. Регулярные выражения (маски)
5. Лингвистические методы (морфология, контентная фильтрация)
6. Ручное детектирование (карантин)

Классификация информационных объектов по требуемой степени безотказности

Параметр	**класс 0**	**класс 1**	**класс 2**	**класс 3**
Максимально возможное непрерывное время отказа	1 неделя	1 сутки	1 час	1 час
В какое время суток продолжительность отказа не может превышать указанное выше ?	в рабочее	в рабочее	в рабочее	24 часа в сутки
Средняя вероятность доступности данных в произвольный момент времени	80%	95%	99.5%	99.9%
Среднее максимальное время отказа	1 день в неделю	2 часа в неделю	20 минут в неделю	12 минут в месяц

Классификация информационных объектов по степени конфиденциальности

Класс	**Тип информации**	**Описание**	**Примеры**
0	открытая информация	общедоступная информация	информационные брошюры, сведения публиковавшиеся в СМИ
1	внутренняя информация	информация, недоступная в открытом виде, но не несущая никакой опасности при ее раскрытии	финансовые отчеты и тестовая информация за давно прошедшие периоды, отчеты об обычных заседаниях и встречах, внутренний телефонный справочник фирмы
2	конфиденциальная информация	раскрытие информации ведет к значительным потерям на рынке	реальные финансовые данные, планы, проекты, полный набор сведений о клиентах, информация о бывших и нынешних проектах с нарушениями этических норм
3	секретная информация	раскрытие информации приведет к финансовой гибели компании	(зависит от ситуации)

Требования по работе с конфиденциальной информацией

При работе с информацией **1-го класса конфиденциальности** рекомендуется выполнение следующих требований :

* осведомление сотрудников о закрытости данной информации,
* общее ознакомление сотрудников с основными возможными методами атак на информацию
* ограничение физического доступа
* полный набор документации по правилам выполнения операций с данной информацией

Требования по работе с конфиденциальной информацией

При работе с информацией **2-го класса конфиденциальности** к перечисленным выше требованиям добавляются следующие :

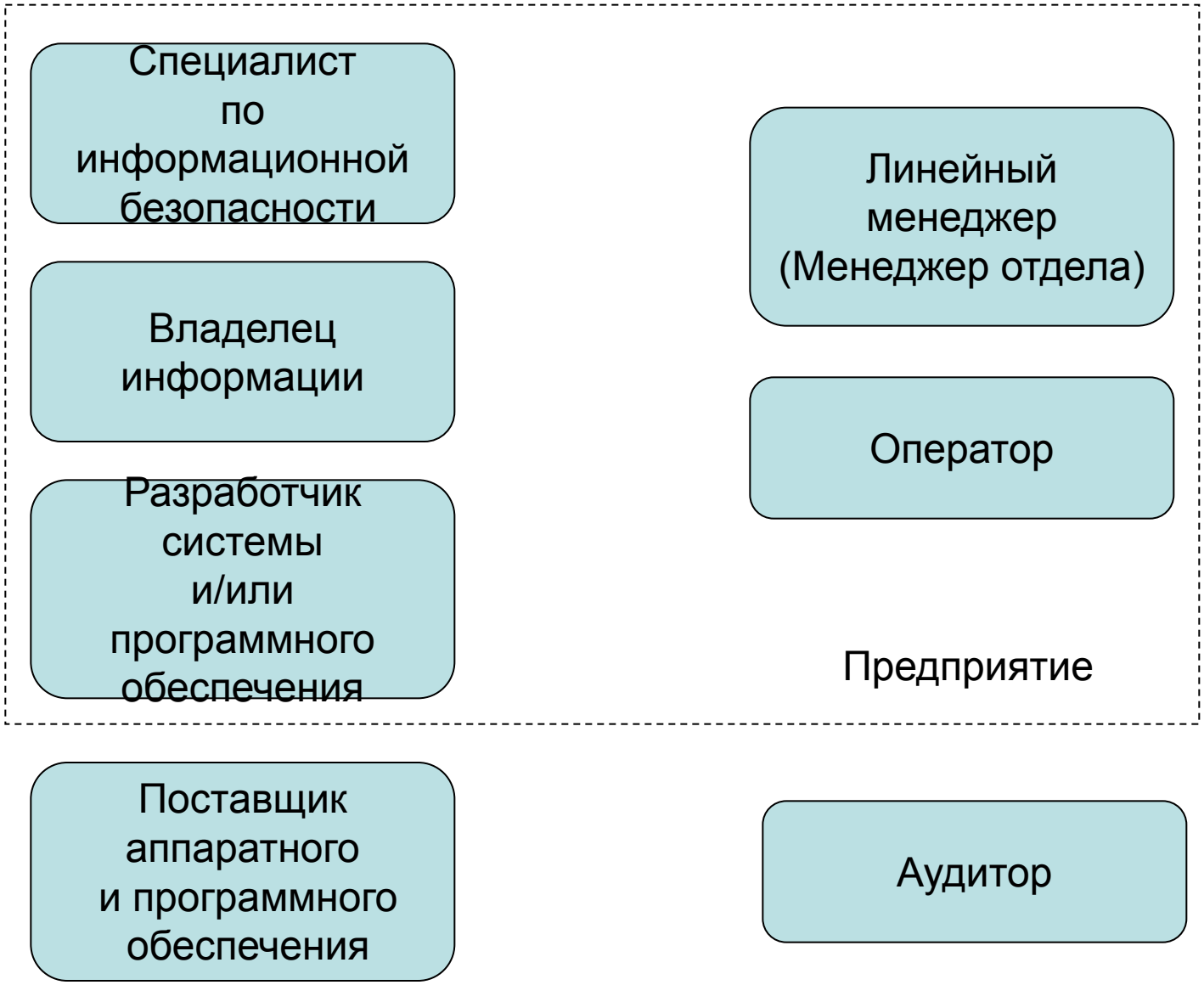
* расчет рисков атак на информацию
* поддержание списка лиц, имеющих доступ к данной информации
* по возможности выдача подобной информации по расписку
* автоматическая система проверки целостности системы и ее средств безопасности
* надежные схемы физической транспортировки
* обязательное шифрование при передаче по линиям связи
* схема бесперебойного питания ЭВМ

Требования по работе с конфиденциальной информацией

При работе с информацией **3-го класса конфиденциальности** ко всем перечисленным выше требованиям добавляются следующие :

* детальный план спасения либо надежного уничтожения информации в аварийных ситуациях (пожар, наводнение, взрыв)
* защита ЭВМ либо носителей информации от повреждения водой и высокой температурой
* криптографическая проверка целостности информации

Политика ролей



Два основополагающих принципа обеспечения оптимальной и безопасной работы пользователей:

- разделение обязанностей и прав доступа;
- минимизация привилегий.

Принцип разделения обязанностей и прав доступа предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Ликвидация системного аккаунта пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале - одновременно с извещением о наказании или увольнении) !

Политика информационной безопасности

Политика безопасности – это документированный комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии. Политика безопасности включает в себя требования в адрес персонала, менеджеров и технических служб.

Основные **направления** разработки политики безопасности :

* определение какие данные и насколько серьезно необходимо защищать,
* определение кто и какой ущерб может нанести фирме в информационном аспекте,
* вычисление рисков и определение схемы уменьшения их до приемлемой величины.

Два подхода к оценке ситуации в области информационной безопасности

«Снизу вверх»

Я – злоумышленник. Мои действия? Как и на что напасть?»

«Сверху вниз»

Я – защищаюсь. Мои действия? Что защищать, как это защищено сейчас?»

Мотивация построения политики информационной безопасности

1. Выполнение требований руководства компании
2. Выполнение требований российского законодательства
3. Выполнение требований клиентов и партнеров
4. Подготовка к сертификации ISO 9001, ISO 15408 и ISO 17799
5. Устранение замечаний аудиторов
6. Получение конкурентного преимущества на рынке
7. Демонстрация заинтересованности руководства компании
8. Создание корпоративной культуры безопасности
9. Уменьшение стоимости страхования
10. Экономическая целесообразность

Успешность политики информационной безопасности

1. Понимание необходимости защиты информации
2. Обучение и информирование сотрудников компании
3. Персональная ответственность каждого сотрудника
4. Юридическая ответственность сотрудников компании
5. Закрепление ответственности сотрудников компании
6. Согласованность во взглядах
7. Создание корпоративной культуры безопасности

Кому и что доверять? Модели доверия…

☺ Доверять всем и всегда

☹ Не доверять никому и никогда

😐 Доверять избранным на время

Примерный состав группы по разработке политики безопасности

Примерный состав группы по разработке политики безопасности

1. Генеральный директор
2. Директор службы автоматизации и информатизации
3. Аналитик в области информационной безопасности
4. Технический специалист
5. Юрист
6. Представители от пользователей

1. Директор
2. Заместитель директора по коммерческим вопросам
3. Начальник информационно-технического отдела
4. Технический специалист
5. Юрист
6. Представители от пользователей

Выдержка из политики безопасности

"Сотрудники несут личную ответственность за безопасность любой информации, используемой и/или сохраненной с применением их учетных записей в компании. Используйте руководство пользователя для получения рекомендаций по защите вашей учетной записи и информации с использованием стандартных методов безопасности на уровне операционной системы или при помощи программного обеспечения шифрования, типа PGP. Конфиденциальная информация компании или сторонних организаций не должна храниться или быть переданной на компьютеры не принадлежащие компании."

Вопросы для анализа ситуации и выработки решений

Что сейчас у нас с резервированием? Как резервировать? Что резервировать? Как определить, что резервировать? Куда резервировать? Сколько это стоит? Насколько это выгодно?

Что самое ценное у нас? Что самое ненадежное у нас? Где корень зла? Где хуже всего мотивация? Насколько страшно для нас то или иное событие? Кто те люди, которые для нас наиболее опасны как сотрудники?

Как жить нашей организации каждый день так, чтобы проблем с информационной безопасностью почти не было? Как описать жизнь в организации для каждой роли так, чтобы все точно знали – как жить в мирное и в военное время?

Что можно исправить достаточно легко, исходя из нынешнего положения вещей? Что чуть сложнее? Что надо купить, чтобы исправить ситуацию? Только ли оборудованием решаются проблемы?

Ущерб от атаки («У») может быть представлен неотрицательным числом в приблизительном соответствии со следующей таблицей :

Величина ущерба	**Описание**
0	Раскрытие информации принесет ничтожный моральный и финансовый ущерб фирме
1	Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты
2	Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются минимально
3	Значительные потери на рынке и в прибыли. От фирмы уходит ощутимая часть клиентов
4	Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы.
5	Фирма прекращает существование

Вероятность атаки («В») представляется неотрицательным числом в приблизительном соответствии со следующей таблицей :

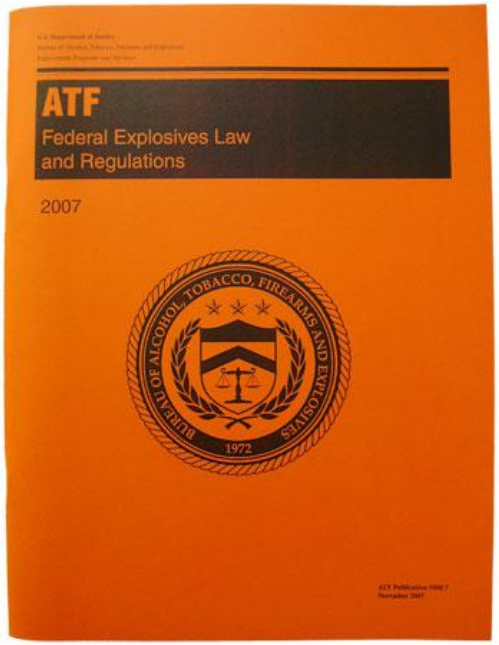
Вероятность	**Средняя частота появления**
0	Данный вид атаки отсутствует
1	реже, чем раз в год
2	около 1 раза в год
3	около 1 раза в месяц
4	около 1 раза в неделю
5	практически ежедневно

Следующим этапом составляется **таблица рисков предприятия**.
Она имеет следующий вид :

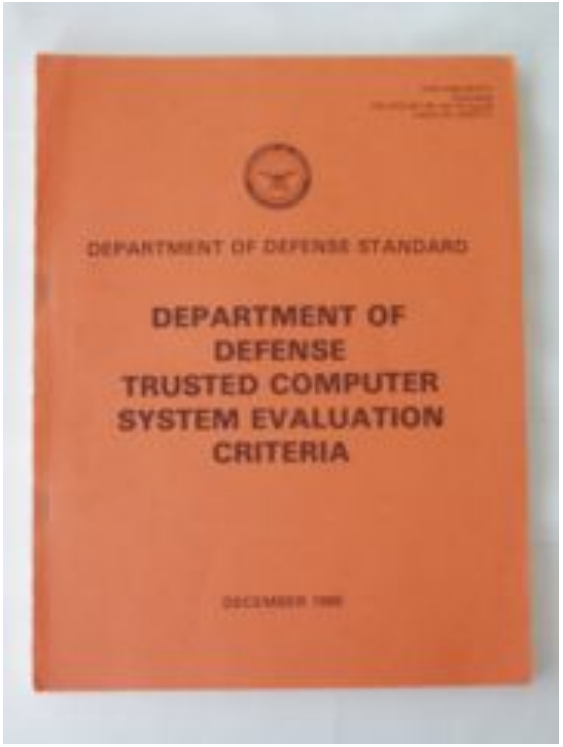
Описание атаки	**Ущерб**	**Вероятность**	**Риск (=Ущерб*Вероятность)**
Спам (переполнение почтового ящика)	1	4	4
Копирование жесткого диска из центрального офиса	3	1	3
...	...	...	…
Итого :			28

Раздел пятый

«Стандарты и спецификации в области информационной безопасности»

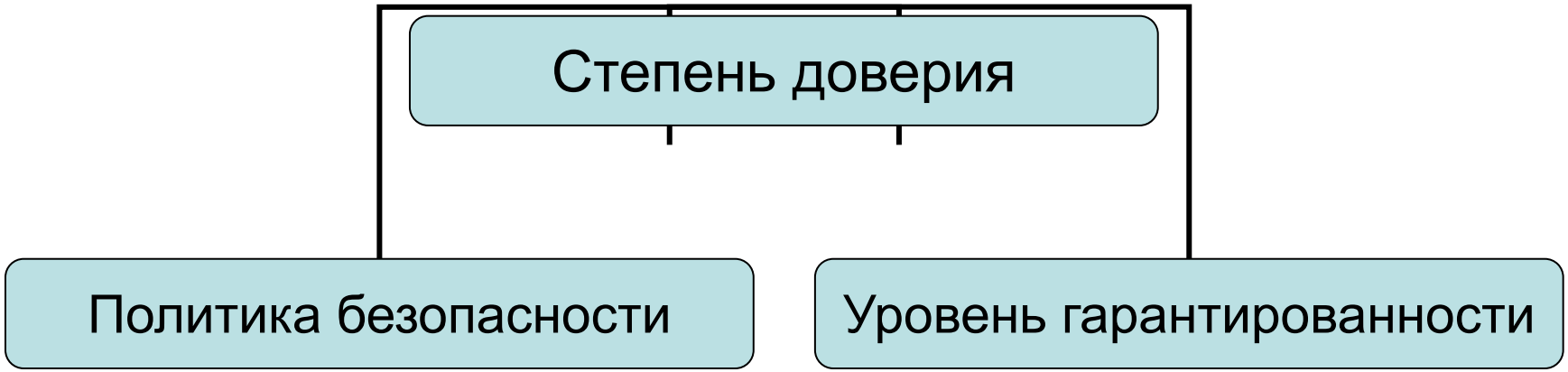


Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США «**Критерии оценки доверенных компьютерных систем**» (Trusted Computer System Evaluation Criteria).
Данный труд, называемый чаще всего по цвету обложки «**Оранжевой книгой**», был впервые опубликован в августе 1983 г.



В «Оранжевой книге» доверенная система определяется как «*система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа*».

Доверенная система – это система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.



Политика безопасности – набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию.

Уровень гарантированности – мера доверия, которая может быть оказана архитектуре и реализации ИС.

Важным средством обеспечения безопасности является механизм *подотчетности* (протоколирования).

Доверенная вычислительная база (ДВБ) – это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жи

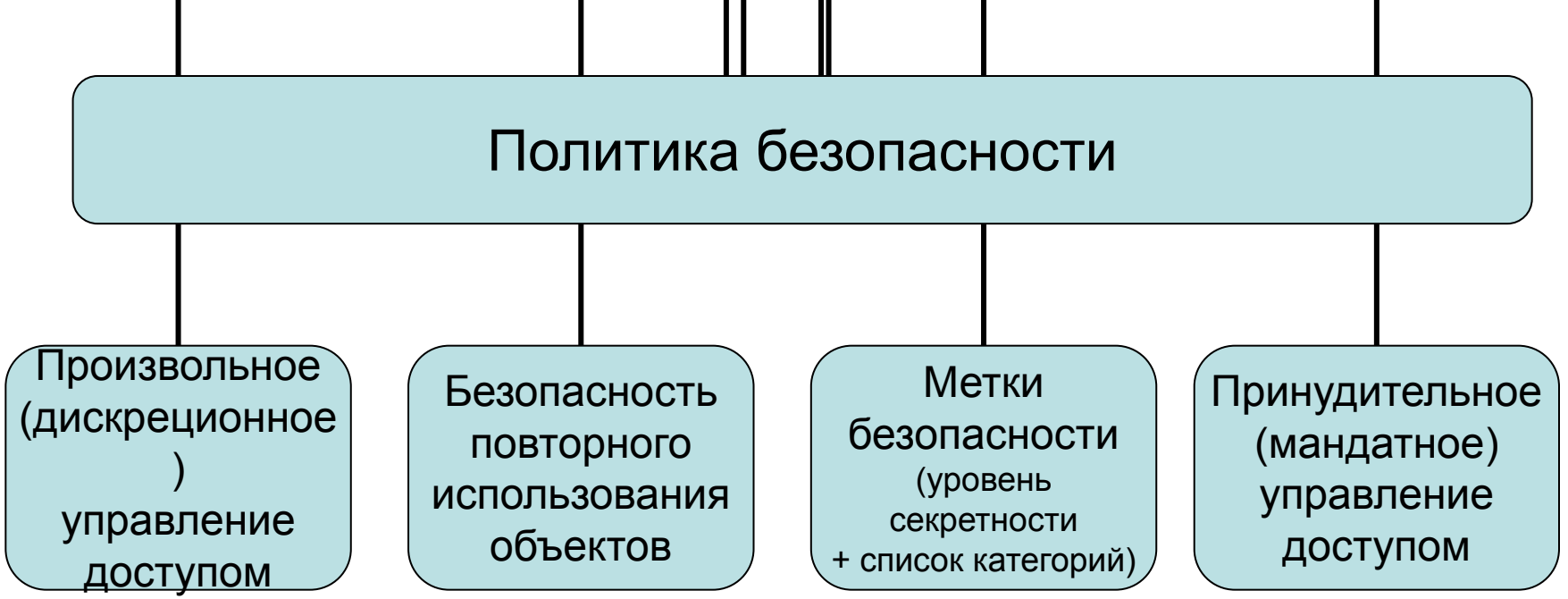
С
выполн

Монитор должен быть компактным, чтобы его можно было проанализировать и протестировать, будучи уверенным в полноте тестирования

•Качест онитора
•Из ованность
•Полнота
•Верифицируемость

Реализация монитора обращений называется **ядром безопасности.**

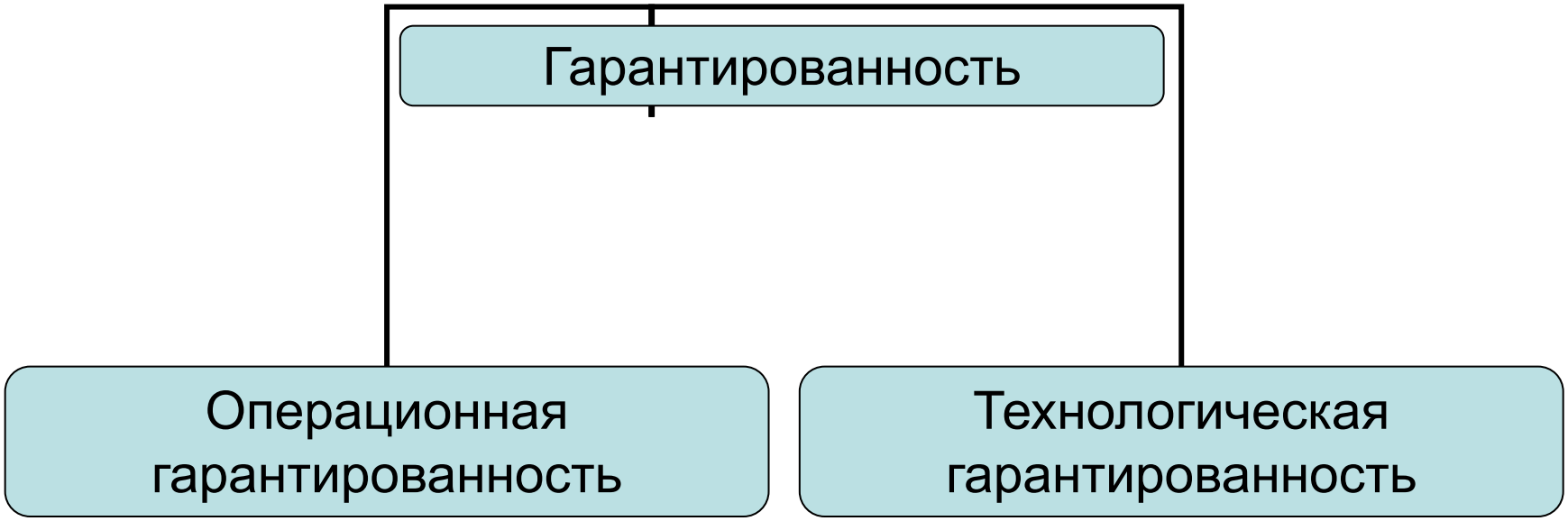
Границу доверенной вычислительной базы называют **периметром безопасности.**



Цель подотчетности – в каждый момент времени знать, кто работает в системе и что делает.

Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.



Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации;
- доверенное администрирование;
- доверенное восстановление после сбоев.

Технологическая гарантированность охватывает весь жизненный цикл системы, т. е. периоды проектирования, реализации, тестирования, продажи и сопровождения. Все перечисленные действия должны выполняться в соответствии с жесткими стандартами, чтобы исключить утечку информации и нелегальные «закладки».

Операционная гарантированность – это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности.

Тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня;

Помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и верификации систем;

Механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;

Должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Должна быть продемонстрирована устойчивость доверенной выч… …опыткам проникновения

C2

B1

B2

B3

A1

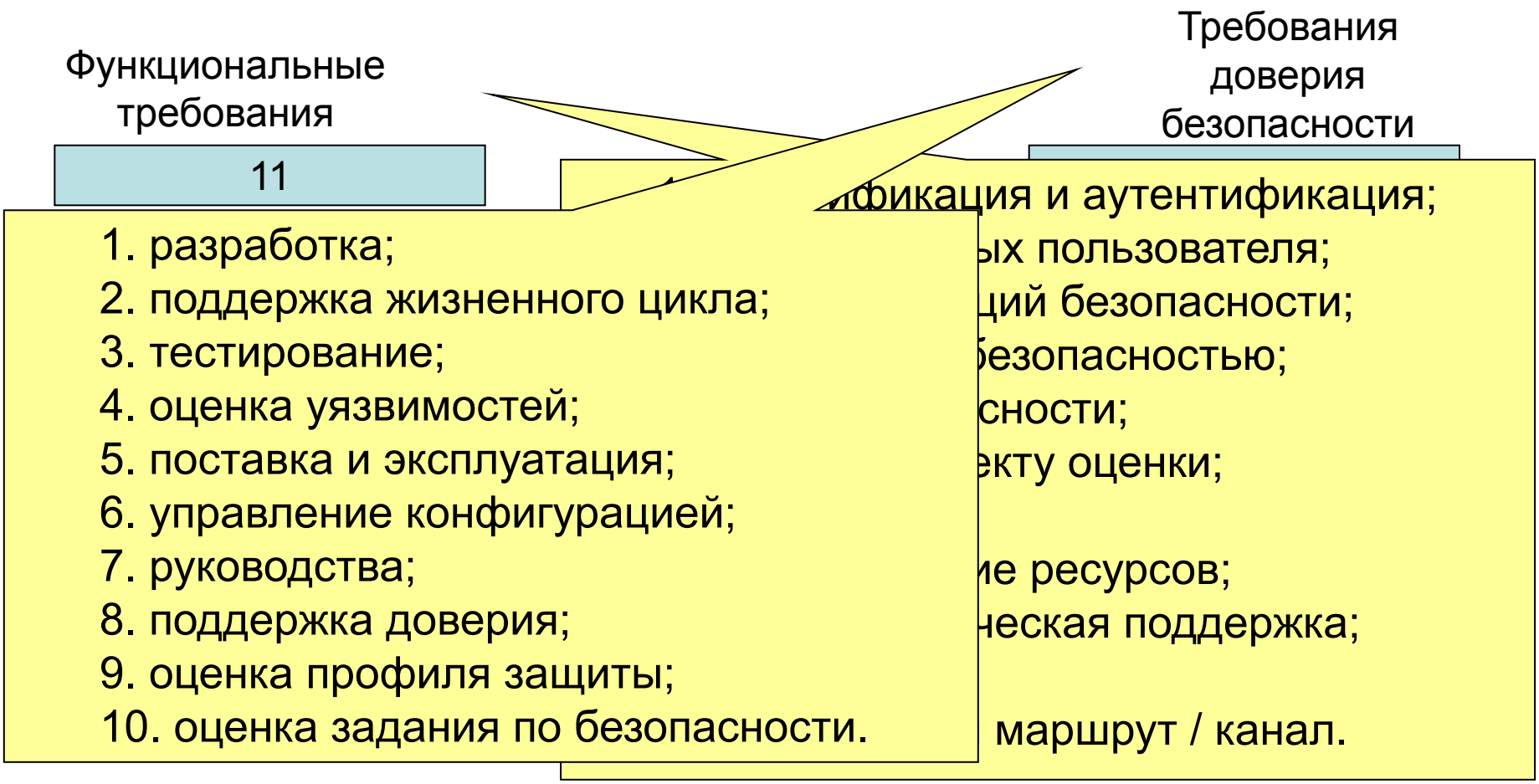
Информационная безопасность распределенных систем. Рекомендации X.800

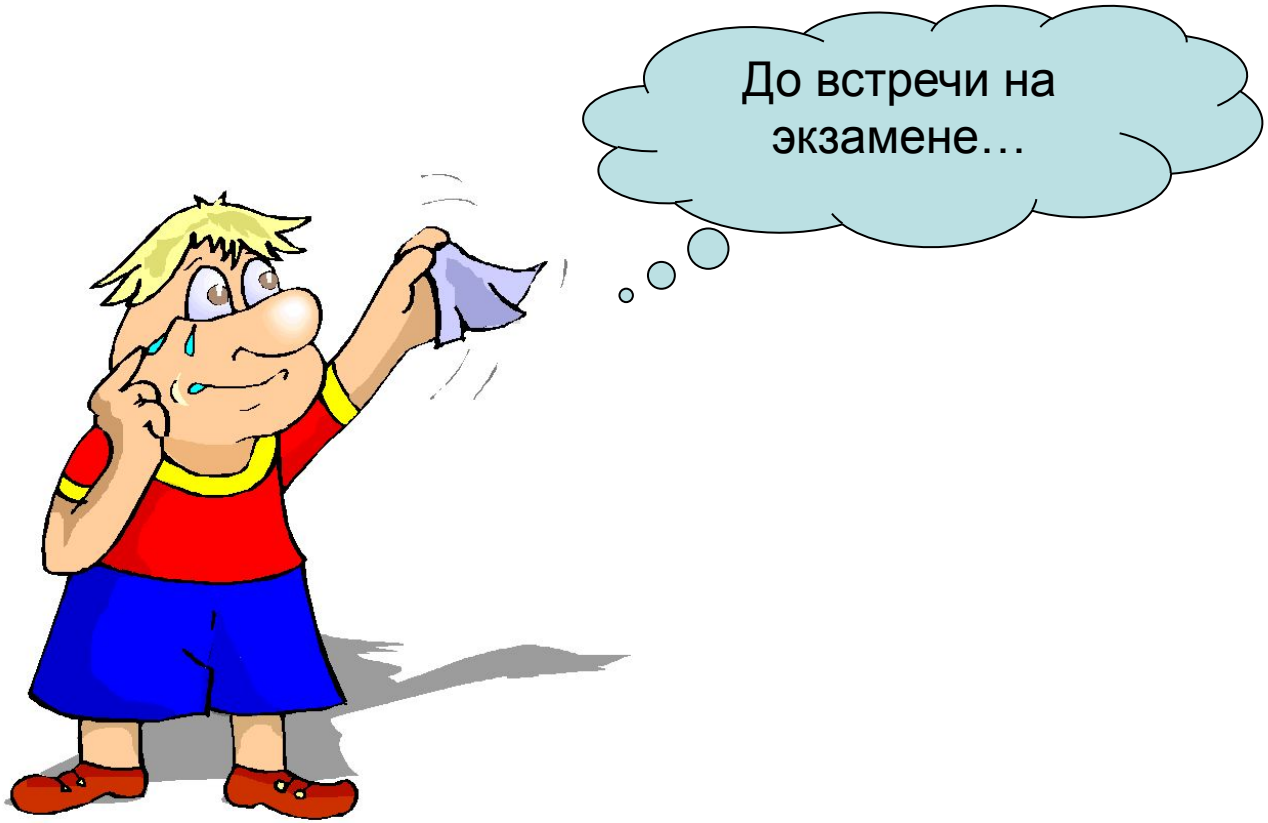
Функции безопасности	**Уровень модели OSI**						
	1	2	3	4	5	6	7
Аутентификация	–	–	+	+	–	–	+
Управление доступом	–	–	+	+	–	–	+
Конфиденциальность соединения	+	+	+	+	–	+	+
Конфиденциальность вне соединения	–	+	+	+	–	+	+
Избирательная конфиденциальность	–	–	–	–	–	+	+
Конфиденциальность трафика	+	–	+	–	–	–	+
Целостность с восстановлением	–	–	–	+	–	–	+
Целостность без восстановления	–	–	+	+	–	–	+
Избирательная целостность	–	–	–	–	–	–	+
Целостность вне соединения	–	–	+	+	–	–	+
Неотказуемость	–	–	–	–	–	–	+

Информационная безопасность распределенных систем. Рекомендации X.800

Функции	Механизмы							
	Шифрование	Электронная подпись	Управление доступом	Целостность	Аутентификация	Дополнение трафика	Управление маршрутизацией	Нотаризация
Аутентификация партнеров	+	+	–	–	+	–	–	–
Аутентификация источника	+	+	–	–	–	–	–	–
Управление доступом	–	–	+	–	–	–	–	–
Конфиденциальность	+		+	–	–	–	+	
Избирательная конфиденциальность	+	–	–	–	–	–	–	–
Конфиденциальность трафика	+	–	–	–	–	+	+	–
Целостность соединения	+	–	–	+	–	–	–	–
Целостность вне соединения	+	+	–	+	–	–	–	–
Неотказуемость	–	+	–	+	–	–	–	+

Стандарт ISO/IEC 15408 **«Критерии оценки безопасности информационных технологий»**




До встречи на экзамене…