

ЭЛЕКТРОННЫЕ ДЕНЬГИ

МИЛЛИОН В ТВОЕМ
КОМПЬЮТЕРЕ

КТО
ЕСТЬ
КТО...

РЫНОК
ЭЛЕКТРОННЫХ
ПЛАТЕЖНЫХ
СИСТЕМ
СТРАНЫ
ФОРМИРУЮТ
НЕСКОЛЬКО
КРУПНЫХ
ИГРОКОВ

СТР. 12

С НИМИ
УДОБНО?

USABILITY-РЕЙТИНГ
ЭЛЕКТРОННЫХ
ПЛАТЕЖНЫХ
СИСТЕМ

СТР. 26

КАРДИНГ
ПО-НОВОМУ

СОВРЕМЕННЫЕ
МЕТОДИКИ
ВЗЛОМА

СТР. 86



Создай свою реальность

с компьютером DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT



Включи DEPO Ego — и перед тобой откроется новая реальность твоих любимых компьютерных игр. Наслаждайся быстротой реакции и скоростью, исследуй распахнувшийся перед тобой мир высококачественной компьютерной графики и настоящего экшена. Теперь эта цифровая реальность может стать твоей благодаря компьютеру DEPO Ego на базе процессора Intel® Pentium® 4 с технологией HT.



DEPO Ego 360 TV:

- процессоры Intel® Pentium® 4 с технологией HT серии 6xx (2Mb cash второго уровня)
- чипсет Intel® 925XE с улучшенной архитектурой
- сверхбыстрая память DDR2
- новые возможности графики PCI-Express
- реалистичный объемный 8-канальный звук

Компания DEPO Computers Тел./факс: (095) 969-2215, www.depo.ru

Intel, Intel Inside, the Intel Inside Logo и Intel Pentium являются зарегистрированными товарными знаками Intel Corporation и её отделений в США и других странах. Microsoft и Windows являются зарегистрированными товарными знаками компании Microsoft и её отделений в США и других странах.



INTRO

Честно признаюсь, что я не особо доллюбливаю платежные системы. Никогда не забуду эйфорию заработанных «фантиков» школьных лет. Фантики казались особенными, явно пахли деньгами (что бы ни говорил Трахтенберг) и отказывались тратиться, так как новые поступления были совершенно непредсказуемы. Но факт остается фактом: наличные деньги были ценнее виртуальных обещаний.

Другое дело, что реальные бумажные деньги имеют и массу недостатков, о которых никто не задумывается, так как люди приспособились ко всем «купюрным» напастям на уровне рефлексов. Прежде всего, наличность нужно постоянно таскать с собой. Чем больше сумма, тем больше проблем с тем, куда засунуть ее. Ну а для продавцов наличный расчет — желаннейший способ оплаты.

Платежные системы в интернете (которые также называют «электронными деньгами»), но если быть точным, это не одно и то же) — еще один способ оплаты товаров и услуг в Сети, доступный в любое время года, в любой день недели, днем и ночью. Основной психологический барьер, отделяющий пользователей от использования e-money, — незнание, которое порождает недоверие. На самом деле все наоборот удобно и безопасно. Обо всех тонкостях и нюансах ты узнаешь из этого Спеца.

Андрей Каролик

содержание №12(61)

ИСПОЛЬЗОВАНИЕ

Как это было	6
История денег	
Электронная история	8
Кто придумал электронную наличность	
Кто есть кто	12
Рынок электронных платежных систем страны формируют несколько крупных игроков	
Кто? Где? Когда?	16
Когда и почему удобнее применять определенную электронную платежную систему	
Особое мнение	18
Какое будущее у электронных денег	
Деньги для эксперта	24
Руководство по платежным интернет-системам для опытного пользователя	
С ними удобно?	26
Usability-рейтинг электронных платежных систем	
Взгляд изнутри	30
Интервью с разработчиками платежных систем	
Старые добрые пластиковые карты	36
Чем пользуются мошенники	
Виртуальный метаболизм	40
Как вывести свою наличность или положить ее на счет — все доступные способы и их безопасность	
Автоматический обменник	44
Roboxchange.com	
Продайся за e-money	46
Или как стать виртуальной рабыней	
Гид по кошелькам	52
Краткая инструкция по использованию платежных интернет-систем	

БЕЗОПАСНОСТЬ

Доверяй, но проверяй	58
Безопасность электронных платежей	
Кража электронных денег	64
Взлом и защита WebMoney	
Чей safe лучше?	70
Рейтинг безопасности электронных платежных систем	
Платить предохраняясь	76
Обеспечение надежного процессинга в электронных магазинах	
Сложный симбиоз	84
Что получится, если скрестить пластиковую карту и WebMoney	
Кардинг по-новому	86
Современные методики взлома	
Атака на смарт-карты	90
Безопасность платежных смарт-карт	



ЭКСПЕРТ НОМЕРА

АНДРЕЙ МЕЖУТКОВ

ИНЖЕНЕР-СИСТЕМОТЕХНИК (ЗАКОНЧИЛ РАДИОТЕХНИЧЕСКИЙ ФАКУЛЬТЕТ УГТУ-УПИ). ЗАНИМАЕТСЯ РАЗЛИЧНЫМИ АСПЕКТАМИ ЗАЩИТЫ ИНФОРМАЦИИ С 1986 ГОДА. ИНТЕРЕСЫ В ОСНОВНОМ СОСРЕДОТАЧИВАЮТСЯ В ОБЛАСТИ АДМИНИСТРАТИВНОГО И ОРГАНИЗАЦИОННО-ПРАВОВОГО РЕСУРСА. В НАСТОЯЩЕЕ ВРЕМЯ — ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ЕКАТЕРИНБУРГСКОГО ФИЛИАЛА ФГУП НТЦ «АТЛАС» ФСБ РОССИИ. ИМЕЕТ ПУБЛИКАЦИИ В СПЕЦИАЛЬНЫХ ИЗДАНИЯХ. АВТОР СДКУРСА «ПРАКТИЧЕСКОЕ РУКОВОДСТВО ПО МЕТОДАМ И СРЕДСТВАМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ», ИЗДАННОГО В КОМПАНИИ DIGITAL SECURITY.

SPECIAL DELIVERY

F.A.Q.	96
Ответы на наиболее часто задаваемые вопросы	
Обзор сайтов	100
Самые вкусные сайты про e-money	
ОФФТОПИК	
NoNaMe	106
Свежий софт от ntm.ru	
Admining	108
Восставший из диска	
Вы хотели ATI?	112
Препарируем Middle-end Radeon'ы	
Plextor PX-716SA	117
Plextor нарежет	
Е-мыло	118
Пишите письма	
STORY	120
Ночная работа	

СПЕЦ

www.xakep.ru

Мнение редакции не всегда совпадает с мнением авторов. Все материалы этого номера представляют собой лишь информацию к размышлению. Редакция не несет ответственности за незаконные действия, совершенные с ее использованием, и возможный причиненный ущерб. За перепечатку наших материалов без спроса — преследуем.

РЕДАКЦИЯ

Главный редактор

Николай «AvaLANche» Черепанов (avalanche@real.xakep.ru)

Выпускающий редактор

Ашот Оганесян (ashot@real.xakep.ru)

Андрей Каролик (andrusha@real.xakep.ru)

Редактор

Александр «Dr. Klouniz» Лозовский (alexander@real.xakep.ru)

DVD/CD/OFFTOPIC

Иван «SkyWriter» Касатенко (sky@real.xakep.ru)

Литературный редактор

Валентина Иванова (valy@real.xakep.ru)

Арт-директор

Иван Васин (vasin@real.xakep.ru)

Дизайнер

Наталья Жукова

Иллюстратор

Иван Величко (vel@shuka.ru)

ЕЖЕМЕСЯЧНЫЙ
ТЕМАТИЧЕСКИЙ
КОМПЬЮТЕРНЫЙ
ЖУРНАЛ
12 (61) ДЕКАБРЬ 2005

РЕКЛАМА

Директор по рекламе ИД (game)land

Игорь Пискунов (igor@gameland.ru)

Руководитель отдела рекламы цифровой группы

Ольга Басова (olga@gameland.ru)

Менеджеры отдела

Ольга Емельянцева (olgaeml@gameland.ru)

Евгения Горячева (goryacheva@gameland.ru)

Оксана Алексина (alekhina@gameland.ru)

менеджер по работе с сетевыми РА, корпоративные продажи

Максим Григорьев (grigoriev@gameland.ru)

Трафик-менеджер

Марья Алексеева (alekseeva@gameland.ru)

тел.: (095) 935.70.34

факс: (095) 780.88.24

РАСПРОСТРАНЕНИЕ

Директор отдела дистрибуции и маркетинга

Владимир Смирнов (vladimir@gameland.ru)

Оптовое распространение

Андрей Степанов (andrey@gameland.ru)

Подписка

Алексей Попов (popov@gameland.ru)

тел.: (095) 935.70.34

факс: (095) 780.88.24

PUBLISHING

Издатель

Сергей Покровский (pokrovsky@gameland.ru)

Учредитель

ООО «Гейм Лэнд»

Директор

Дмитрий Агарунов (dmitri@gameland.ru)

Финансовый директор

Борис Скворцов (boris@gameland.ru)

ГОРЯЧАЯ ЛИНИЯ ПО ПОДПИСКЕ

тел.: 8 (800) 200.3.999

Бесплатно для звонящих из России

для ПИСЕМ

101000, Москва,

Главпочтамт, а/я 652, Хакер Спец

spec@real.xakep.ru

http://www.xakep.ru

Отпечатано в типографии «ScanWeb», Финляндия

Зарегистрировано в Министерстве Российской Федерации

по делам печати, телерадиовещанию

и средствам массовых коммуникаций

ФИ № 77-12014 от 4 марта 2002 г.

Тираж 42 000 экземпляров.

Цена договорная.

CD:

КОПИШЬ НА FERRARI? ТОГДА КОПИ В ИНТЕРНЕТ-ВАЛЮТЕ! ЗАОДНО ТЫ СМОЖЕШЬ МГНОВЕННО НАХОДИТЬ ЕЙ ВЫГОДНОЕ ПРИМЕНЕНИЕ И ЗАРАБАТЫВАТЬ ЕЩЕ БОЛЬШЕ, ПРОДВИГАЯСЬ К СВОЕЙ МЕЧТЕ. А ЧТОБЫ ЭТУ ВАЛЮТУ НЕНАРОКОМ НЕ УВЕЛИ ;), ПОЛЬЗУЙСЯ СОФТОМ С ДИСКА И ЖИВИ СПОКОЙНО!

Спец 10(59), Мобильный взлом
Обновления для Windows за месяц

БЕЗОПАСНОСТЬ

AVP 5.0.388
Agnitum Outpost Firewall Pro 3.0
Agnitum Outpost Firewall Pro 3.0 (RU)
BestCrypt 7.20 (Linux/Win32)
DrWeb 4.33 + ключ на месяц!
DriveCrypt Plus 3.0
IMsecure Pro 1.5
Kaspersky Anti-Hacker 1.8.180
PGP 9.0
ZoneAlarm 6.0 Free
ZoneAlarm Anti-Spyware 6.1
ZoneAlarm Antivirus
ZoneAlarm Internet Security Suite 6.0
ZoneAlarm Pro 6.0

СОФТ НА КАЖДЫЙ ДЕНЬ

Konfabulator 2.1.1
Mozilla FireFox 1.5rc2 (RU)
Mozilla FireFox 1.5rc3
Mozilla Thunderbird 1.0.7
Opera 8.50
TheBat! 3.62
WebMoney 2.4.0.3
Интернет.Кошелек 2.1.0.3

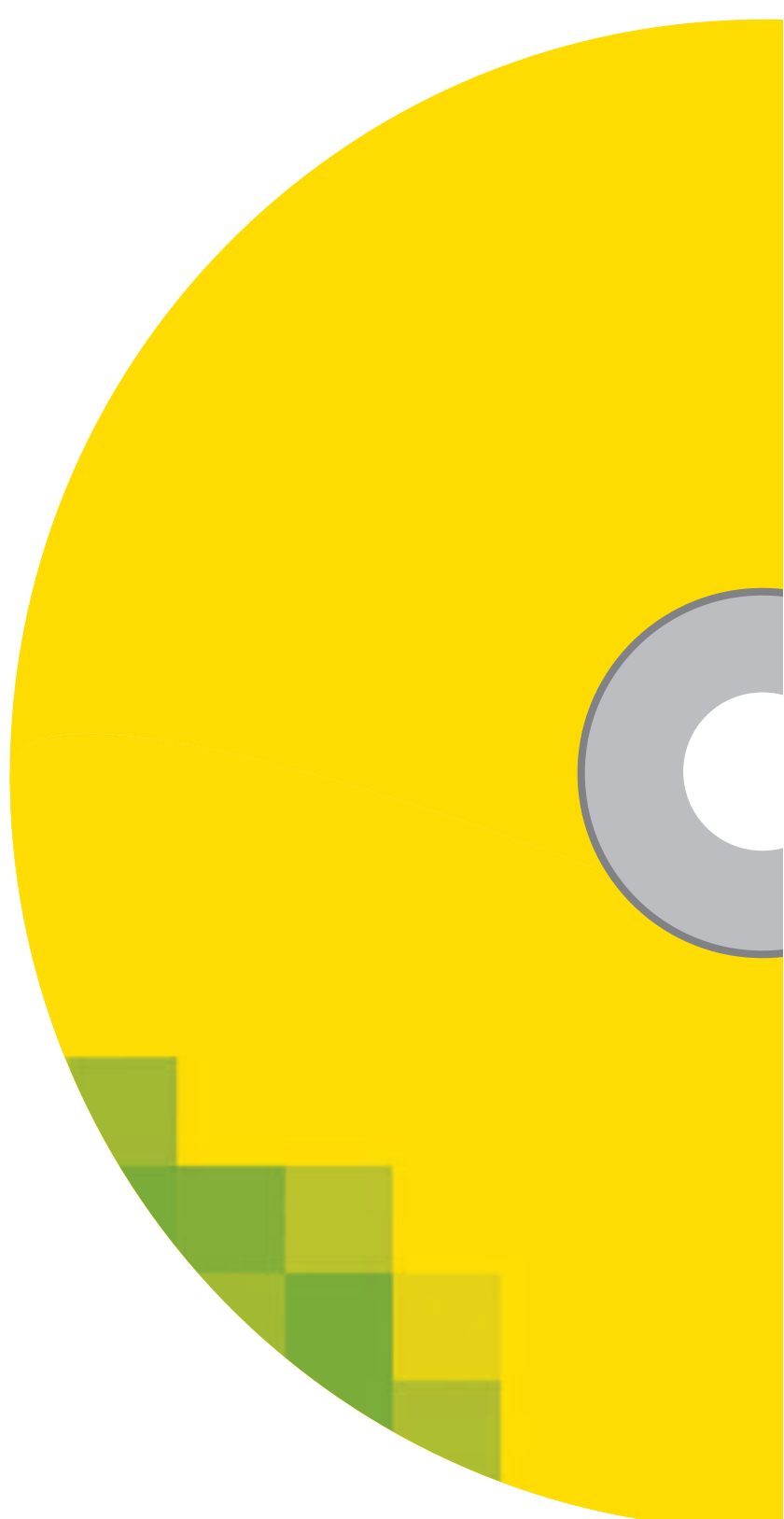
ВИРТУАЛЬНАЯ ЖИЗНЬ

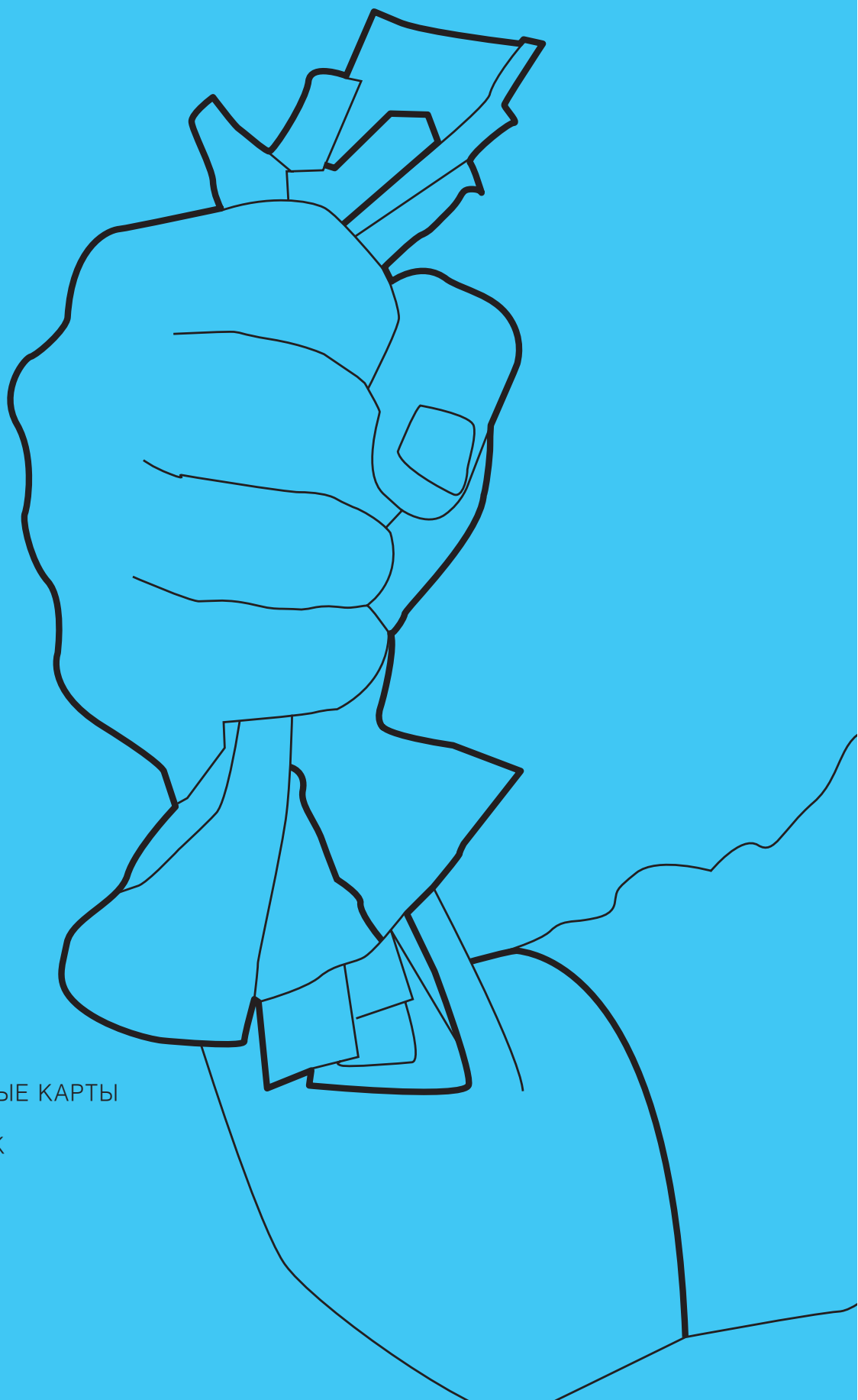
Microsoft Virtual PC 2004 SP1
VMWare Workstation 4.5.2

СОФТ ОТ NONAME

AveDesk 1.3
Batch Watermark Creator 3.2
F-Secure Anti-Virus Client Security 6
LimeWire v4.9
MidBut Pro 1.10 Beta
Netobjects Fusion 8
NikSaver 1.4
RegDoctor 1.42
Screen Flash Professional 1.62
TagScanner 4.9
TaskSwitchXP 2.0

ВСЕ ЭТО НА МУЛЬТИЗАГРУЗОЧНОМ CD!





ИСПОЛЬЗОВАНИЕ

КАК ЭТО БЫЛО
ЭЛЕКТРОННАЯ ИСТОРИЯ
ЖЕЛЕЗО
КТО ЕСТЬ КТО
КТО? ГДЕ? КОГДА?
ОСОБОЕ МНЕНИЕ
ДЕНЬГИ ДЛЯ ЭКСПЕРТА
С НИМИ УДОБНО?
ВЗГЛЯД ИЗНУТРИ
СТАРЫЕ ДОБРЫЕ ПЛАСТИКОВЫЕ КАРТЫ
ВИРТУАЛЬНЫЙ МЕТАБОЛИЗМ
АВТОМАТИЧЕСКИЙ ОБМЕННИК
ПРОДАЙСЯ ЗА E-MONEY
ГИД ПО КОШЕЛЬКАМ



как это было

ИСТОРИЯ ДЕНЕГ

ЧТО ТАКОЕ ЭЛЕКТРОННЫЕ ДЕНЬГИ И ОТКУДА ОНИ ПОЯВИЛИСЬ? ЧТОБЫ ОТВЕТИТЬ НА ЭТОТ ВОПРОС, НУЖНО РАЗОБРАТЬСЯ, ЧТО ТАКОЕ ДЕНЬГИ, ПОЭТОМУ СНАЧАЛА ПРОВЕДЕМ НЕБОЛЬШОЙ ЭКСКУРС В ИСТОРИЮ ДЕНЕГ | ДЕНИС КОЛИСНИЧЕНКО

3-2
тыс. лет до н.э.

Появление, по сути, первых банков. Их функции выполняли храмы и дворцы, в которых хранились товары. Когда именно появились первые деньги, сказать весьма сложно. В разные времена функции денег выполняли совершенно разные вещи. Сначала был товарный обмен — то, что сейчас называется бартером, например определенное количество рыбы обменивается на определенное количество мяса. Затем в качестве денег стали использовать слитки различных цветных металлов, раковины, жемчуг. Особое место, конечно, занимало золото.

640-630
гг. до н.э.

Впервые появились деньги в нашем обычном понимании. Это произошло в Лидии (современная территория Турции) — уже не в виде слитков металлов или товаров, а в виде круглых монет из сплава серебра и золота).

600
г. до н.э.

Появился безналичный расчет. Торговцы и путешественники стали перевозить с собой не деньги, а расписки банка Тифия, который был расположен в Греции. Самое интересное, что уже тогда этот банк напоминал современные банки тем, что имел сеть филиалов в разных городах Греции, в том числе в городах Ионийских островов. Китайцы оказались скупее греков и чеканили монеты из железа. Первые китайские монеты появились приблизительно в то же время, что и греческие.

910
год

Начало массового выпуска бумажных денег в Китае. Оказывается, китайцы — самые продвинутые банкиры. Однако станок для печати денег был изобретен лишь через 500 лет — в 1440 году. Иоганн Гуттенберг создал станок для печати книг, который позже был использован для печати денег. Впрочем, нужно отметить, что ранее в Китае использовалось подобие печатного станка, но все же это было несколько не то.

1649
год

Появляются чеки в современном понимании этого слова. Чеки начали выпускать банки Англии, Франции, Голландии. Немного позже, в 1661 году, появился первый в мире государственный центральный банк.

1824
год

Создание первой системы безналичного расчета за товары и услуги. А через 13 лет — в 1837 году — был изобретен телеграфный аппарат, который в конце XIX века стал использоваться для осуществления финансовых операций. В начале XX века 80% мировых банковских платежей проходили через телеграфный перевод.

В Университете Пенсильвании создан первый компьютер — ENIAC (Electronic Numerical Integrator and Calculator), который весил «всего лишь» 30 тонн, а стоил намного больше, чем весил. Через семь лет на конференции в Бреттон-Вудсе было принято решение о создании Международного валютного фонда (International Monetary Fund) Всемирного Банка (World Bank) и развитии свободной торговли.

В США создана первая в мире централизованная электронная сеть учета банковских чеков. Появление этой сети стало возможным благодаря созданию сети ARPANET по заказу Министерства Обороны США в 1969 году. Уже в 1973 году 239 банков из 15-ти различных стран мира создают Общество всемирной межбанковской финансовой телекоммуникации (Society for Worldwide Interbank Financial Telecommunication — SWIFT). Система SWIFT полностью заменила телеграф, который до этого использовался в финансовых операциях.

Появление первой электронной платежной системы DigiCash. Позже на ее основе начался выпуск смарт-карт (хотя сама технология была запатентована еще в 1974 году). Смарт-карточки использовались везде, где требовалась оплата: телефонные аппараты (таксофоны), метро и т.д. Когда деньги на смарт-карте заканчивались, пользователь или выбрасывал карту, или пополнял счет на ней.

Банк международных расчетов опубликовал первые официальные исследования по электронным деньгам, в которых была рассмотрена идея эмиссии электронных денег Центральным банком. Также в этом году ассоциация VISA создала свой электронный кошелек VISA Cash. Сразу после этого Euro-pay, VISA и MasterCard заявляют о разработке единых требования к микропроцессорным картам (спецификация EMV, название по первым буквам компаний-разработчиков).

Создана система PayPal, позволяющая пользователям пересылать друг другу деньги с помощью электронной почты. А в Европе примерно в это же время была создана система PhonePaid, позволяющая управлять банковским счетом с помощью мобильного телефона.

Роберт Мандел (Robert Mandell), лауреат Нобелевской премии по экономике, высказал свое предположение о том, что в 2040 году будет создана единая валюта, основой которой станут доллар США, евро и йена (денежная единица Японии), соответственно, и электронные деньги станут универсальными и едиными.

1840
ГОД1937
ГОД1950
ГОД1972
ГОД1991
ГОД1993
ГОД1995
ГОД1996
ГОД1997
ГОД1998
ГОД1999
ГОД2003
ГОД

Появление госбанка в России. Любопытно, что госбанк США (Федеральная резервная система) появился лишь через 73 года (!) — в 1913 году. До появления ФРС американские банки сами выпускали доллары, которые отличались друг от друга по размеру и дизайну.

Появление первой кредитной карточки — Diners Club. Правда, это была несколько не та кредитная карточка, которой мы все пользуемся сейчас. Diners Club была предназначена только для оплаты завтраков, обедов и ужинов в ресторанах, то есть не была универсальной. Универсальная же карта была выпущена Национальным банком Франклина два года спустя.

В лаборатории CERN был разработан протокол WWW, первоначально предназначенный для обмена информацией среди ученых-физиков. Ровно через год после этого открылись первые сайты банков: сначала банки публиковали на сайтах только рекламную информацию, но затем появились полноценные интернет-представительства банков. Уже в то время было подсчитано, что стоимость транзакции, проведенной через интернет, на 90% дешевле аналогичной транзакции, совершенной в обычном филиале.

90% всех банковских платежей уже совершаются в электронной форме. Подсчитано, что 3 трлн. транзакций совершалось в электронной форме, 1 трлн. — чеками, а 0,2 трлн. — наличными. Компания Mondex разрабатывает первый электронный многовалютный кошелек, испытания которого успешно прошли в Англии. В этом же году компания Proton выпустила многовалютную карточку, которая стала использоваться для мелких покупок, а Банк им. Марка Твена начал эмиссию «цифровых наличных» по системе DigiCash.

VISA и MasterCard разработали протокол SET (Secure Electronic Transaction — протокол безопасных электронных транзакций), который используется для транзакций через интернет. В этом же году протокол SET был запущен в работу.

Осуществлены первые транзакции в единой европейской валюте — евро. А через год — в 2000 — 12 производителей микропроцессорных карт и соответствующего программного обеспечения заявили о разработке первого универсального «электронного кошелька»



электронная ИСТОРИЯ

КТО ПРИДУМАЛ ЭЛЕКТРОННУЮ НАЛИЧНОСТЬ

НЕСМОТРЯ НА ТО, ЧТО ТЕРМИН «ЭЛЕКТРОННЫЕ ДЕНЬГИ» ПОЯВИЛСЯ СРАВНИТЕЛЬНО НЕДАВНО И ПОКА УПОТРЕБЛЯЕТСЯ НЕ ШИРОКО, ИСТОРИЯ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ НАСЧИТЫВАЕТ УЖЕ НЕМАЛО ЛЕТ И ЗАСЛУЖИВАЕТ ВНИМАНИЯ. ЧТОБЫ ПОНЯТЬ, ИЗ ЧЕГО И КАК ВЫРОСЛИ ЭЛЕКТРОННЫЕ ДЕНЬГИ, РАЗОБЬЕМ ИХ ИСТОРИЮ НА ЧЕТЫРЕ ОСНОВНЫХ ЭТАПА | [Дмитрий Денежко aka denga \(denezko@dmity.ru\)](mailto:denezko@dmity.ru)

первый этап Идея расчетов с помощью предоплаченных карт появилась более 125-ти лет назад в далеком 1880 году. Именно тогда известный американский ученый Эдвард Беллами в своей книге «Смотря назад» (Looking Backwards) предложил использовать предоплаченные карты при расчетах. Однако его перспективная идея не нашла отклика. Через почти четверть века в 1914 году предпринимаются первые попытки применить кредитные карты, тем не менее, все заканчивается неудачей. В результате больше 35-ти лет ничего принципиального с идеей электронных денег не происходит.

В 1950 году компания DCI (Diners Club International) выпустила первую в мире платежную карту — Diners Club. Вслед за этим, уже на следующий год после проявления инициативы DCI, американский банк Franklin National Bank выпустил первую кредитную карту. Еще через семь лет вновь американский банк, крупнейший в стране Bank of America, выпускает первую универсальную банковскую

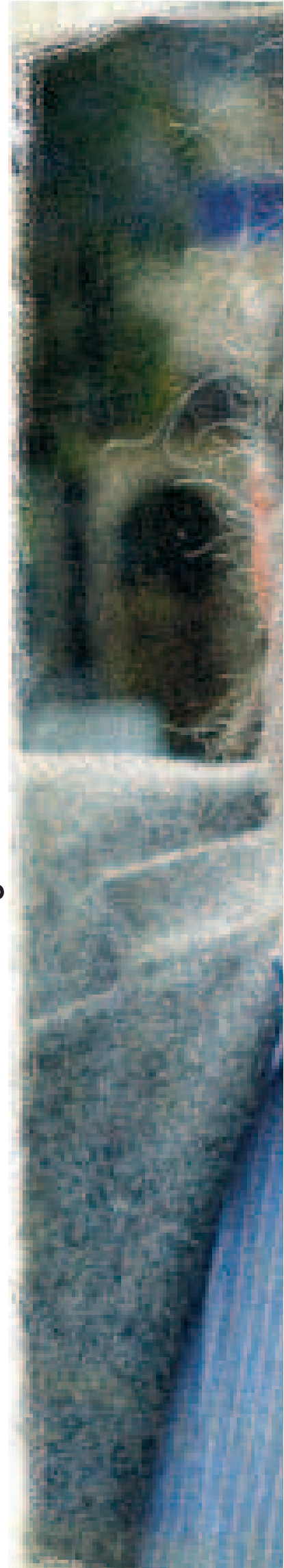
карточку BankAmericard, которая сейчас известна всему миру под названием Visa. Уже в 1965 году образована первая межбанковская карточная ассоциация — Eurocard International.

Серьезный конкурент Visa появился только через восемь лет. В 1966 году все крупные банки Калифорнии приступили к эмитированию Master Charge (позднее MasterCard). Так протекал некий вводный этап истории электронных платежных систем, следующий же период связан с развитием информационных технологий и их применением в банковской сфере.

второй этап Вторая половина XX века запомнилась истории бурным развитием информационных технологий и микроэлектроники в частности. Американские банки, снова впервые в мире, на-

ПЕРВАЯ КРЕДИТНАЯ
БАНКОВСКАЯ КАР-
ТОЧКА В СОВЕТС-
КОМ СОЮЗЕ БЫЛА
ВЫПУЩЕНА «ВНЕШ-
ЭКОНОМБАНКОМ»
В 1988 ГОДУ

Дэвид Чаум — «отец»
всех электронных пла-
тежных систем



обнищавший родитель

ДЕВИД ЧАУМ ОСНОВАЛ КОМПАНИЮ DIGICASH В 1990 ГОДУ. В ЕЕ ОСНОВЕ, КАК ТЫ УЖЕ ЗНАЕШЬ, ЛЕЖАЛА ТЕХНОЛОГИЯ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ, А ТОЧНЕЕ ДАЖЕ ЕЕ КОНКРЕТНОЕ ПРОГРАММНОЕ ВОПЛОЩЕНИЕ — ECASH. ИНТЕРЕС К ЭТОЙ СИСТЕМЕ НЕУКЛОННО РОС, И УЖЕ В 1994 ГОДУ ДЕВИДУ ЧАУМУ УДАЛОСЬ СОЗДАТЬ ДОСТАТОЧНО КРУПНУЮ СЕТЬ БАНКОВ, АКТИВНО ПРИМЕНЯЮЩИХ ДАННОЕ РЕШЕНИЕ. В ЧАСТНОСТИ, В ЭТУ СЕТЬ ВХОДИЛИ ТАКИЕ КРУПНЫЕ ИГРОКИ, КАК: ADVANCE BANK OF AUSTRALIA, DEUTSCHE BANK, MARK TWAIN BANK, DEN NORSKE BANK И BANK AUSTRIA. ВСЕ ОНИ СТАЛИ ЭМИТИРОВАТЬ ЭЛЕКТРОННУЮ НАЛИЧНОСТЬ.

ОДНАКО, НЕСМОТЯ НА АМБИЦИИ И МНОГООБЕЩАЮЩИЙ СТАРТ, ТОГДА ТЕХНОЛОГИЯМ И МЕЧТАМ, СВЯЗАННЫМ С НЕЮ, НЕ СУЖДЕНО БЫЛО СБЫТЬСЯ. ПРОШЛО ТРИ ГОДА — ШЕЛ 1997 — НО ВСЕ ЭТИ ПРОЕКТЫ ПО-ПРЕЖНЕМУ ОСТАВАЛИСЬ В ОПЫТНОЙ ЭКСПЛУАТАЦИИ, А СТАДИЯ ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ НИЧУТЬ НЕ ПРИБЛИЖАЛАСЬ. В РЕЗУЛЬТАТЕ БАНКИ РЕШИЛИ РЕОРГАНИЗОВАТЬ ДЕЯТЕЛЬНОСТЬ В ОБЛАСТИ ЭЛЕКТРОННОЙ НАЛИЧНОСТИ. ОДНАКО ЭТИ МЕРЫ ЛИШЬ УСУГУБИЛИ СИТУАЦИЮ. ПОСЛЕДНИМ УДАРОМ ОКАЗАЛОСЬ ЗАЯВЛЕНИЕ УПРАВЛЕНЦЕВ MERCANTILE BANCORP (ПОГЛОТИВШЕГО К ТОМУ МОМЕНТУ MARK TWAIN BANK) О ТОМ, ЧТО «5000 ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ ECASH НЕ СОЗДАЛИ ЗАМЕТНОГО ПОТОКА КАПИТАЛОВ». ФИНАНСОВАЯ СТРУКТУРА ПРЕКРАТИЛА УЧАСТИЕ В ПРОЕКТЕ DIGICASH. ОТКАЗЫ ПОСЫПАЛИСЬ ОДИН ЗА ДРУГИМ, И ВСКОРЕ DIGICASH ОБЪЯВИЛА О СВОЕМ БАНКРОТСТВЕ.

ТЕХНОЛОГИЯ ECASH СТАЛА ФУНДАМЕНТОМ ПЕРВОЙ В МИРЕ ЭЛЕКТРОННОЙ ПЛАТЕЖНОЙ СИСТЕМЫ DIGICASH И ПРАРОДИТЕЛЕМ ВСЕХ СУЩЕСТВУЮЩИХ СЕГОДНЯ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

КРЕДИТНЫЕ КАРТОЧКИ СИСТЕМЫ VISA INTERNATIONAL ПРИШЛИ В НАШУ СТРАНУ ЛИШЬ ЧЕРЕЗ 20 ЛЕТ ПОСЛЕ ПОЯВЛЕНИЯ ИХ НА ЗАПАДЕ

чинают активно внедрять электронные методы переводов денежных средств. Появляются технологии электронных переводов, такие как EFT (Electronic Funds Transfer). В 1968 году свет увидела технология электронного обмена данных — Electronic Data Interchange (EDI), которая была впоследствии положена в основу электронных транзакций. Электронные платежи развиваются все активнее, мир начинает относиться к кредитным карточкам без панического страха. В США формируются две межбанковские карточные ассоциации. Первая из них, NBI, известна сейчас как Visa International, вторая — ICA, соответственно MasterCard International.

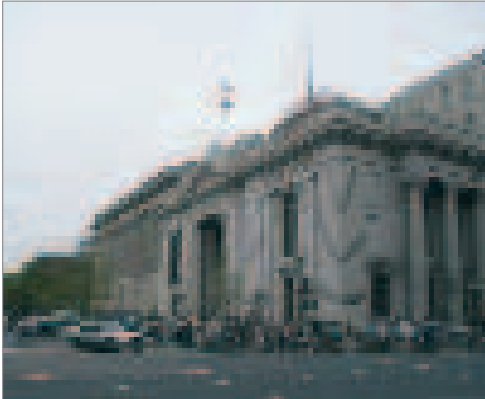
1974 год стал в каком-то смысле переломным в плане американского господства в становлении электронных платежей: именно в этом году Роберт Морено во Франции регистрирует патент на технологию изготовления смарт-карт. США, правда, не отстают, и уже через год, в 1975 году, в Штатах появляются первые банковские автоматы для получения наличных — банкоматы.

Информационные технологии не стояли на месте, и уже в 1979 году в Америке для безналичных банковских платежей начато применение первых электронных терминалов, которые были названы EFTPOS и заложили основы электронных платежей.

Уже в 1984 году предприятия финансового сектора начинают активно применять электронную почту при общении с клиентами. По сути, это был первый шаг на пути к электронному банкингу и интернет-банкингу. Проходит еще три года, и первые банки начинают предоставлять услуги в режиме онлайн.

Приблизительно в это же время в историю электронных денег вступает и наша страна (тогда СССР). В 1988 году «Внешэкономбанк» СССР выпускает первую в государстве кредитную банковскую карточку — Eurocard Gold. Впрочем, такую карту могли получить только особо важные персоны: на всю огромную территорию СССР было выпущено около 30-ти этих карт. Классическая Visa пришла в нашу страну намного позже, лишь в 1991 году: спустя почти 20 лет после появления карт Visa и MasterCard за рубежом российский «Кредо-банк» выпустил первую в стране международную кредитную банковскую карточку системы Visa International.

В общем, именно второй этап заложил основы для систем электронных платежей с помощью кредитных банковских карт. Третий же этап отличился развитием информационных технологий.



ВОПРОСЫ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ ПО-ПРЕЖНЕМУ ОСТАЮТСЯ ОСНОВНОЙ ПРИЧИНОЙ, ПО КОТОРОЙ ЛЮДИ НЕ БРОСАЮТСЯ ПОГОЛОВНО К ЦИФРОВОЙ НАЛИЧНОСТИ



Первые банкоматы появились 30 лет назад в США

1995 год был богат на знаковые события истории электронных платежных систем. К примеру, бельгийская компания Proton первой в мире ввела в обращение моновалютную микропроцессорную карточку для мелких покупок, английская компания Mondex провела разработку первого в мире «электронного кошелька». Кошелек, разумеется, был моновалютный, но ценен собственно прецедент.

третий этап В 1981 году создан первый классический персональный компьютер — IBM PC, а развитие микроэлектроники к тому времени начало прямо бурлить. Во второй половине 80-х годов в пластиковую кредитную карточку удалось вмонтировать микропроцессор, что предопределило появление принципиально нового вида денег — цифровой наличности. Однако реально революционным для истории электронных денег становится 1993 год, в котором доктор Дэвид Чаум, глава группы криптографии в голландском национальном исследовательском центре CWI, разработал программное решение — технологию eCash для работы с цифровой наличностью.

Более 50-ти лет назад Bank of America выпустил первую в мире Visa

НАША СТРАНА СТАРАЛАСЬ НЕ ОТСТАВАТЬ ОТ МИРА В РАЗВИТИИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В СФЕРЕ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ. УЖЕ В 1998 ГОДУ БАНК «ТАВРИЧЕСКИЙ» ОБЪЯВИЛ О РАЗРАБОТКЕ РОССИЙСКОГО АНАЛОГА ЦИФРОВОЙ НАЛИЧНОСТИ

Впоследствии eCash стала фундаментом первой в мире электронной платежной системы DigiCash и прародителем всех существующих сегодня электронных платежных систем. Тем не менее, попав под реорганизацию, компания DigiCash Inc. обанкротилась, а лицензия на технологию eCash была продана. В чем же состояла суть новой революционной технологии?

Концепция eCash вводила в обиход понятие электронной валюты для оплаты товаров и услуг через компьютерные сети, которые к тому времени уже получили значительное распространение. Сама валюта хранится на жестком диске персонального компьютера, куда она закачивается с помощью специального клиентского программного обеспечения, которое необходимо предварительно установить. Принципы осуществления электронных платежей за прошедшие 12 лет не претерпели принципиальных изменений, разве что многие современные e-money-системы позволяют осуществлять платежи не устанавливая специальное клиентское программное обеспечение на свой компьютер.

Через год после появления eCash, в 1994 году, в США была осуществлена первая в истории покупка через интернет. В этом же году в России появилась первая отечественная микропроцессорная карта системы «Золотая Корона». Технология eCash стремительно набирала популярность во всем мире, и в 1995 году система на ее основе получила ежегодную премию Европейской комиссии по информационным технологиям (Information Technology European Award (ITEA'95)). Такая высокая награда присуждается в номинации технологического новаторства, соответственно, изобретение доктора Чаума можно считать революционным. После первого тестирования и экспериментов лицензию на технологию eCash купили восемь крупных финансовых институтов, а американский банк Mark Twain Bank первым в мире приступил к эмиссии «цифровых наличных» по технологии DigiCash. В том же 1995 году, если верить данным Федеральной резервной системы США, уже 90% совокупной стоимости всех транзакций Америки производилось в электронной форме.

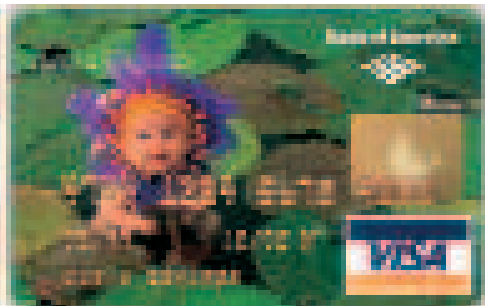
был разработан специальный протокол для осуществления безопасных транзакций в интернете — Secure Electronic Transaction (SET).

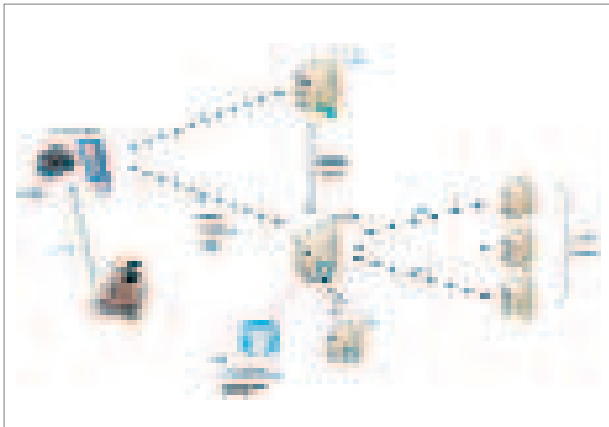
В 1997 году в Сингапуре ассоциацией Visa International произведена первая транзакция с помощью SET.

Успешная операция была замечена прогрессивными финансовыми институтами: в США открыт первый в мире виртуальный банк, предоставляющий все банковские услуги через интернет, учредителем «первенца» стал американский банк Cardinal Bank Shares. Россия также старается не отставать от мирового прогресса, в 1998 году отечественным банком «Таврический» сообщено о разработке российского аналога цифровой наличности.

Именно так выглядела первая Visa (слева). А так она выглядит сейчас

В 2000 году ассоциация из 12-ти крупнейших производителей микропроцессорных карт, специализированного программного обеспечения и кре-





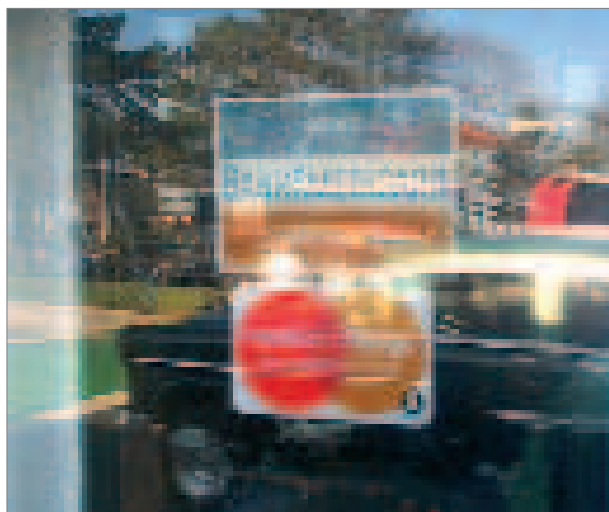
Приблизительно так выглядит использование EFTPOS сегодня

дитных ассоциаций, объявляет о создании первого универсального электронного кошелька, после этого дальнейшее развитие электронных денег практически полностью связано со стремительным вхождением интернета в нашу жизнь.

четвертый этап Уже можно просто подвести некоторые итоги. В современном мире активно работает несколько десятков электронных платежных систем, самые известные из них E-Gold, PayPal, PayPal и StormPay. В России зарубежные системы не так развиты, но хорошие позиции занимают отечественные компании WebMoney, Cyberplat, E-Port, «Яндекс.Деньги», «Рапида». Не так давно крупнейший почтовый сервер России Mail.ru запустил совместно с ИК «Финам» свой проект электронный платежной системы — MoneyMail.

Большинство современных платежных систем, как зарубежных, так и российских, сегодня может функционировать полностью через web-интерфейс, не требуя установки клиентского программного обеспечения. Электронные день-

Витрина прогрессивного американского магазина середины XX века: к оплате принимаются карты BankAmericard и MasterCard, прототипы современных Visa и MasterCard



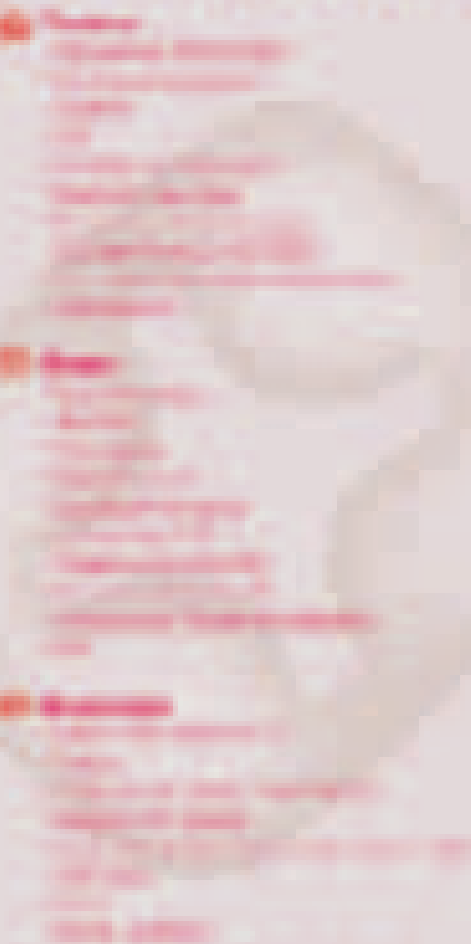
ПЕРВАЯ МЕЖБАНКОВСКАЯ КАРТОЧНАЯ АССОЦИАЦИЯ БЫЛА ОБРАЗОВАНА 40 ЛЕТ НАЗАД. ОНА ПОЛУЧИЛА НАЗВАНИЕ EUROCARD INTERNATIONAL

ПЕРВАЯ В МИРЕ ПЛАТЕЖНАЯ КАРТА БЫЛА ВЫПУЩЕНА СВЫШЕ 55-ТИ ЛЕТ ТОМУ НАЗАД

ги прочно вошли в повседневную жизнь современного человека. Тем не менее, их развитие задерживает, например, государственная политика, связанная с информационной безопасностью, и т.п.

Ряд платежных систем, например российский Cyberplat, кроме различных криптографических алгоритмов, для обеспечения безопасности своих транзакций активно применяет и электронную цифровую подпись. Однако безопасность электронных платежей по-прежнему остается основной причиной, по которой люди не бросаются поголовно к цифровой наличности. В то же время в некоторых странах, например в Сингапуре, уже ведут работы по приданию электронным деньгам статуса законного платежного средства, поэтому электронная наличность может фактически приобрести статус бессрочного обязательства государства и стать обязательной к приему всеми субъектами государства наравне с другими возможными платежными средствами.

ЖУРНАЛ О КОМПЬЮТЕРНОЙ ЖЕЛЕЗЕ



ВЫПУСК № 10



№ 10



ЖЕЛЕЗО

КТО ЕСТЬ КТО...

РЫНОК ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ СТРАНЫ ФОРМИРУЮТ НЕСКОЛЬКО КРУПНЫХ ИГРОКОВ

МЫ ТОЛЬКО УСПЕЛИ ПРИВЫКНУТЬ К КРЕДИТНЫМ КАРТОЧКАМ, И ВОТ ПОСТОЯННО РАЗВИВАЮЩИЙСЯ IT-МИР ПРЕДЛАГАЕТ НАМ НОВОЕ СРЕДСТВО ЭЛЕКТРОННОЙ КОММЕРЦИИ — ЭЛЕКТРОННЫЕ ДЕНЬГИ | ДЕНИС КОЛИСНИЧЕНКО (DHSILABS@MAIL.RU)

Электронные деньги — это несколько усовершенствованный вариант кредитной карточки, но вместо банкомата используется твой компьютер, а вместо самой кредитной карточки — твои файлы сертификатов (или хотя бы имя пользователя и пароль, в зависимости от платежной системы). Принципы использования электронных денег остались теми же, что и для средств на кредитках:

- для САМОСТОЯТЕЛЬНОГО ПОПОЛНЕНИЯ СВОЕГО СЧЕТА ИДЕШЬ В БАНК, НЕЗАВИСИМО ОТ ТОГО, ЧЕМ ПОЛЬЗУЕШЬСЯ, — КРЕДИТКОЙ ИЛИ ЭЛЕКТРОННЫМ КОШЕЛЬКОМ. ОДНАКО ЭЛЕКТРОННЫЕ КОШЕЛЬКИ МОЖНО ПОПОЛНЯТЬ И ПРЕДОПЛАЧЕННЫМИ КАРТАМИ, ПОЧТОВЫМ ПЕРЕВОДОМ ИЛИ В ОФИСЕ КОМПАНИИ, СОЗДАВШЕЙ ПЛАТЕЖНУЮ СИСТЕМУ.
- ИСПОЛЬЗУЯ ЭЛЕКТРОННЫЙ КОШЕЛЕК, КАК И ПРИ ПРИМЕНЕНИИ КРЕДИТКИ, ТЫ МОЖЕШЬ ПОЛУЧАТЬ ДЕНЬГИ ОТ ДРУГИХ УЧАСТНИКОВ СИСТЕМЫ, ДЛЯ ЭТОГО КТО-ЛИБО ДОЛЖЕН ОТПРАВИТЬ ДЕНЬГИ С КАРТОЧКИ И/ИЛИ ЭЛЕКТРОННОГО КОШЕЛЬКА НА ТВОЮ КАРТОЧКУ ИЛИ КОШЕЛЕК. Я НАПИСАЛ «И/ИЛИ», ТАК КАК ВОЗМОЖНЫ ДВУСТОРОННИЕ ОБМЕНИ КАРТОЧКА-КОШЕЛЕК, КОШЕЛЕК-КОШЕЛЕК.

таблица 1. Оборот основных платежных систем

Платежная система	Ввод денег	Вывод денег
WebMoney	0,8%	0,8%
Яндекс.Деньги	БЕСПЛАТНО	3% (+10 РУБЛЕЙ ЗА БЕЗНАЛИЧНЫЙ БАНКОВСКИЙ ПЕРЕВОД)
CyberPlat	С ПОЛЬЗОВАТЕЛЕЙ КОМИССИЯ НЕ ВЗИМАЕТСЯ	С ПОЛЬЗОВАТЕЛЕЙ КОМИССИЯ НЕ ВЗИМАЕТСЯ
E-port	0,5% ПРИ ПОПОЛНЕНИИ СЧЕТА У ДИЛЕРОВ ИЛИ 1,5%+0,01\$ ПРИ ПОПОЛНЕНИИ STB-КАРТОЙ.	1,25-3% ПРИ ПОЛУЧЕНИИ В КАССЕ E-PORT ИЛИ 1% ЗА БАНКОВСКИЙ ПЕРЕВОД.
MoneyMail (Деньги@Mail.ru)	1-3% (ЗАВИСИТ ОТ БАНКА)	1-3% (ЗАВИСИТ ОТ БАНКА)
Рапид	ПЛАТЕЖИ И ПЕРЕВОДЫ — 3%, С ОДНОГО USERID НА ДРУГОЙ — 0,5%	ПЛАТЕЖИ И ПЕРЕВОДЫ — 3%, С ОДНОГО USERID НА ДРУГОЙ — 0,5%
КредитПилот	БЕСПЛАТНО	3% (КОМИССИЯ БАНКА)

- ВЫВОД ДЕНЕГ (ПОЛУЧЕНИЕ НАЛИЧНЫХ) С КОШЕЛЬКА ТАК ЖЕ ПРОСТ, КАК И С КАРТОЧКИ. МОЖНО ОТПРАВИТЬ ДЕНЬГИ НА КАРТОЧКУ И СНЯТЬ ИХ В БЛИЖАЙШЕМ БАНКОМАТЕ, ОТПРАВИТЬ ИХ ПОЧТОВЫМ ПЕРЕВОДОМ ИЛИ ПО WESTERN UNION.
- В ГАРАНТИЯХ БЕЗОПАСНОСТИ ОБА СРЕДСТВА НА ОДИНАКОВОМ УРОВНЕ. ПОЛЬЗОВАТЕЛЬ КРЕДИТКИ — ПОТЕНЦИАЛЬНАЯ ЖЕРТВА ДЛЯ ПРЕСТУПНИКОВ, ПРОМЫШЛЯЮЩИХ ВОЗЛЕ БАНКОМАТОВ. ЕСЛИ ТЫ ПОЛЬЗУЕШЬСЯ ЭЛЕКТРОННЫМ КОШЕЛЬКОМ, РИСКУЕШЬ СТАТЬ ЖЕРТВОЙ ВИРТУАЛЬНОГО ПРЕСТУПНИКА, КОТОРЫЙ ГДЕ-ТО ЕСТЬ, НО ДЛЯ ТЕБЯ НЕВИДИМ. ХОТЯ ЕСЛИ СОБЛЮДАТЬ ЭЛЕМЕНТАРНЫЕ ПРАВИЛА БЕЗОПАСНОСТИ, В ОБОИХ СЛУЧАЯХ ВСЕ БУДЕТ ОК.
- для УПРАВЛЕНИЯ СЧЕТОМ И ЭЛЕКТРОННОГО КОШЕЛЬКА, И КРЕДИТКИ ИСПОЛЬЗУЕТСЯ ТЕРМИНАЛ. В СЛУЧАЕ С КРЕДИТНОЙ КАРТОЙ — БАНКОМАТ, В СЛУЧАЕ С КОШЕЛЬКОМ — КОМПЬЮТЕР С СООТВЕТСТВУЮЩИМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ. ПОЛЬЗОВАТЬСЯ БАНКОМАТОМ ПРОСТО, А КОМПЬЮТЕРОМ — УДОБНО. ДЛЯ ТЕХ, КТО СОВСЕМ НЕ УМЕЕТ РАБОТАТЬ НА КОМПЬЮТЕРЕ, ЭЛЕКТРОННЫЙ КОШЕЛЕК — НЕПОЗВОЛИТЕЛЬНАЯ РОСКОШЬ, В ТО ВРЕМЯ КАК НИ ДЛЯ СРЕДНЕКВАЛИФИЦИРОВАННОГО ПОЛЬЗОВАТЕЛЯ, НИ ДЛЯ ВЫСОКО КВАЛИФИЦИРОВАННОГО НЕТ НИКАКИХ СЛОЖНОСТЕЙ В ЭТОМ ДЕЛЕ — НУЖНО РАЗОБРАТЬСЯ ВСЕГО С ОДНОЙ ПРОГРАММОЙ.

Соответственно, электронные деньги — не такое зло, как кажется многим: они мало отличаются от кредитных карточек, пользоваться ими удобно — банкомат находится прямо у тебя дома. Правда, этот банкомат односторонний, ты можешь только отправить деньги, а за наличкой придется куда-то идти. С другой стороны, банкоматы не позволяют отправлять деньги с одной кредитной карточки на другие карты, счет или кошелек — для этого обязательно нужно присутствовать в отделении банка. Посещать данное заведение придется до тех пор, пока компьютеры не получат официальное право на эмиссию денег, а печать они осуществляют успешно уже сейчас.

таблица 2. Тарифы основных платежных систем

Платежная система	Структура	Валюта
WebMoney	ИНТЕРНЕТ-КОШЕЛЕК	РУБЛЬ, ДОЛЛАР, ЕВРО, УКРАИНСКАЯ ГРИВНА, УЗБЕКСКИЙ СУМ
Яндекс.Деньги	ИНТЕРНЕТ-КОШЕЛЕК	РУБЛЬ
CyberPlat	ДИЛЕРСКАЯ СЕТЬ, САЙТ	РУБЛЬ
E-port	ДИЛЕРСКАЯ СЕТЬ, ВИРТУАЛЬНАЯ КАРТА	РУБЛЬ
MoneyMail (Деньги@Mail.ru)	САЙТ	РУБЛЬ, ДОЛЛАР, ЕВРО
Рапид	САЙТ И USERID	РУБЛЬ
КредитПилот	ДИЛЕРСКАЯ СЕТЬ, ВИРТУАЛЬНЫЙ СЧЕТ	РУБЛЬ

**CYBERPLAT — ЭТО
ЕДИНСТВЕННАЯ
СИСТЕМА, ГДЕ
НУЖНО УКАЗЫВАТЬ
СВОИ РЕАЛЬНЫЕ
ДАННЫЕ. НИКАКОЙ
АНОНИМНОСТИ,
ВСЕ КАК В БАНКЕ**

Идея современных электронных денег принадлежит Дэвиду Чауму. В 1993 году этот человек разработал средство eCash, которое позже легло в основу DigiCash. Работать с eCash было очень просто: клиент вносил денежный залог, а потом с помощью специального программного обеспечения управлял своим электронным кошельком. Принципы, положенные в основу eCash, сегодня используются практически всеми современными платежными системами.

Основная цель электронных денег — экономить финансы и время пользователей. Транзакция в электронной платежной системе стоит дешевле, чем традиционная банковская операция. Кроме того, на оформление транзакции электронного кошелька нужны считанные секунды, в то время как на традиционную транзакцию может не хватить и часа: пока доберешься до банка, пока выстоишь в очереди, а время — деньги. Плюс тебе не нужно тратить свое время на походы по магазинам, вместо этого заходишь в интернет-магазин, выбираешь и оплачиваешь товар, через определенное время курьер доставляет его прямо к тебе домой.

Если поискать, то в интернете можно найти очень много различных платежных систем, но на рынке стран СНГ в основном используются следующие системы:

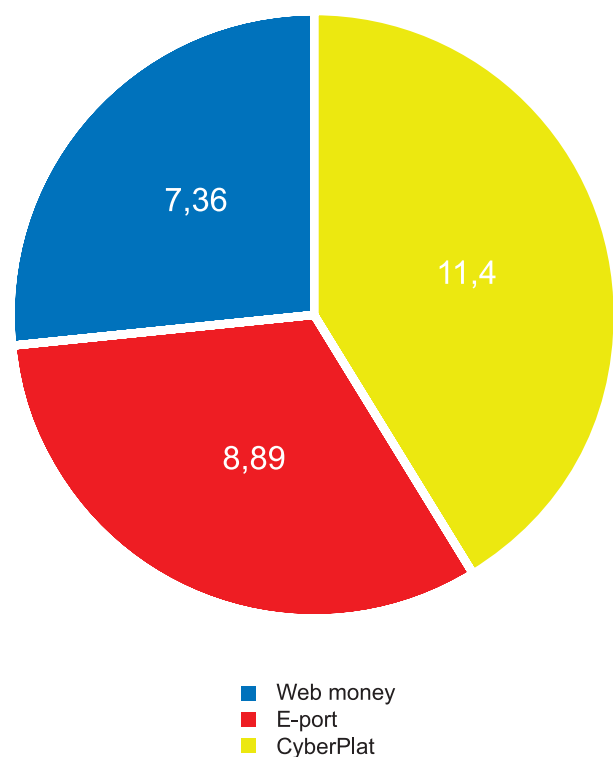
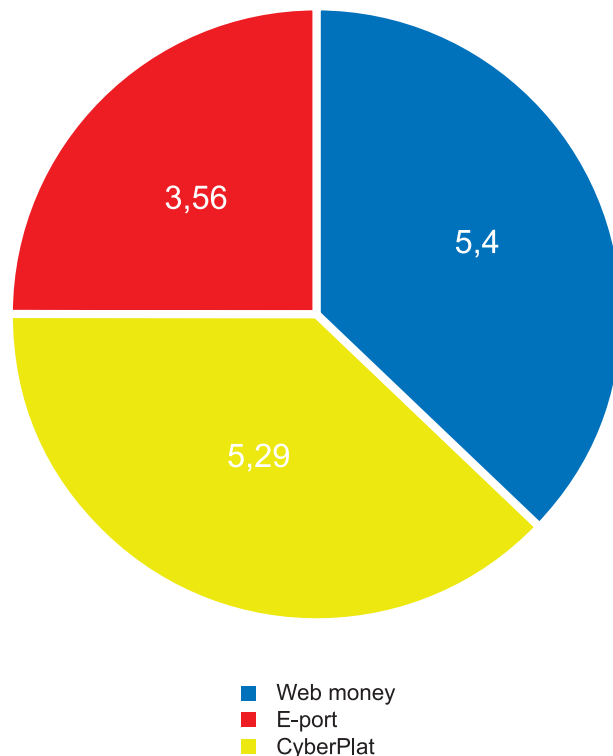
- WEBMONEY
- «ЯНДЕКС.ДЕНЬГИ»
- MONEYMAIL
- CYBERPLAT
- E-PORT
- «РАПИДА»
- «КРЕДИТПИЛОТ»

Структура этих систем различается, поэтому они получают прибыль из разных источников, например основной доход CyberPlat и e-port приходится на дилерскую сеть, WebMoney и «Яндекс.Деньги» — на обычных интернет-пользователей. Но суть не в этом. Для стран СНГ значительны четыре только что названных системы. Посмотрим на табл. 1, где приведены сведения об обороте трех крупнейших систем: CyberPlat, WebMoney и E-port.

Как видишь, за год E-port обошла WebMoney, которой теперь принадлежит только третье место. Но почему? Сравним тарифы E-port и WebMoney. В

перевод на \$1 000 000? легко!

ЛЮБОПЫТНЫЙ ФАКТ: СОВРЕМЕННЫЕ ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ ОБЛАДАЮТ ПОДЧАС ОПРЕДЕЛЕННЫМИ ФИНАНСОВЫМИ ПРЕИМУЩЕСТВАМИ ПО СРАВНЕНИЮ С ТРАДИЦИОННЫМИ ФИНАНСОВЫМИ ИНСТИТУТАМИ. А В СОЧЕТАНИИ С ВОЗМОЖНОСТЬЮ АНОНИМНОЙ РАБОТЫ В ЭЛЕКТРОННОЙ ПЛАТЕЖНОЙ СИСТЕМЕ ЭТО НЕ РЕДКО ДАЕТ ОЧЕНЬ И ОЧЕНЬ ЛЮБОПЫТНЫЙ ИНСТРУМЕНТ. ТАК, НАПРИМЕР, В WEBMONEY ТЕОРЕТИЧЕСКИ НИЧЕГО НЕ МЕШАЕТ ПРОВЕСТИ ХОТЬ \$1 000 000 ЗА ГРАНИЦУ. НАПОМНИМ, ЧТО РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО ПОЗВОЛЯЕТ БЕЗ ОСОБЫХ МУЧЕНИЙ ПЕРЕВОЗИТЬ НЕ БОЛЕЕ \$10 000. В WEBMONEY С ТОЧКИ ЗРЕНИЯ КОНТРОЛИРУЮЩИХ ОРГАНОВ ТЫ СОВЕРШАЕШЬ ДВЕ СДЕЛКИ: ОБМЕН ДЕНЕГ НА ТИТУЛЬНЫЕ ЗНАКИ WEBMONEY В ОДНОЙ СТРАНЕ И ОБРАТНЫЙ ОБМЕН НА ДЕНЬГИ В ДРУГОЙ. ОСТАЕТСЯ ТОЛЬКО ВООРУЖИТЬСЯ ЗНАНИЯМИ, КАК ПРОВЕСТИ ЭТУ ОПЕРАЦИЮ ПО БУХГАЛТЕРСКОЙ И НАЛОГОВОЙ ОТЧЕТНОСТИ, ПОЛУЧИТЬ ПЕРСОНАЛЬНЫЙ АТТЕСТАТ — И ВПЕРЕД!



на диаграммах сверху вниз:

Оборот электронных платежных систем в России за первое полугодие 2004 и 2005 года

службе WebMoney стоимость каждой транзакции (комиссия системы) составляет 0,8%. В E-port стоимость ввода ниже: 0,5% при пополнении счета у дилеров E-port и 1,5%+\$0,01 при пополнении STB-картой. Комиссия за вывод средств составляет 1,25-3% при получении в кассе E-port или 1% за банковский перевод. Как видишь, дело не в тарифах. Скорее всего, пользователям, привыкшим к сберкассам, понравилась сеть филиалов системы E-port, в которых можно получить деньги. Не хочешь или не можешь идти на почту или в банк — иди в кассу E-port, переплати совсем немного и уйди счастливый с деньгами. По сравнению с WebMoney, цена вывода средств в E-port немного завышена, но ничего не поделаешь: дилерскую сеть нужно содержать, и на это требуются деньги.

Если мы заговорили о тарифах, рассмотрим таблицу, в которой сравниваются тарифы всех популярных в России платежных систем (табл. 2).

Посмотри внимательно на табличку и скажи, почему у CyberPlat самые большие обороты. Да-да, именно потому что ввод/вывод денег для обычных пользователей, которые работают с системой через сайт, бесплатен. А система живет за счет комиссионных, которые взимают с дилеров (поставщиков) — 2-5%.

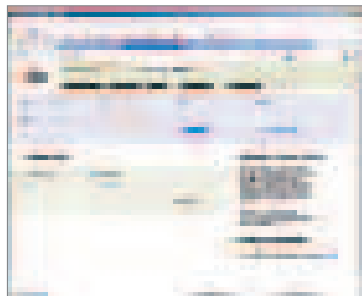
Если разговор завернул в направлении внутренней структуры самих платежных систем, то посмотрим на табл. 3, в которой указана внутренняя структура каждой системы.

Теперь все встало на свои места: мы знаем, где дилерская сеть, а где сайт. Обрати внимание на «Яндекс.Деньги» и «КредитПилот». В первом случае — интернет-кошелек, во втором — дилерская сеть и виртуальный счет. Тарифы примерно одинаковые. Так почему «Яндекс.Деньги» популярнее? В борьбу вступает маркетинг, нужно отдать должное маркетологам компании, которые продвинули «Яндекс.Деньги» несмотря на то, что в народе системы с дилерскими представительствами популярнее, чем интернет-кошельки. Благодаря их усилиям «Яндекс.Деньги» сегодня занимает неплохую позицию на рынке России. Думаю, если бы эта служба научилась работать с долларом и евро, то укрепил бы свои позиции дополнительно.

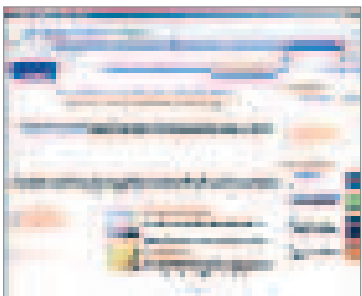
какую систему выбрать В первую очередь оцени тарифы системы. Для тебя это не главное? Тогда нужно определить, что главное. Надежность? Все системы в одинаковой степени надежны, иначе они прекратили бы свое существование, но я рекомендую обращаться к «старожилам» — WebMoney или CyberPlat. Первая появилась на рынке России в 1998 году, вторая еще раньше — в 1997.

Возможно, ты захочешь использовать CyberPlat. Надежная система, на рынке давно, отличные тарифы. Для тебя, как для конечного пользователя, все бесплатно. Однако есть одна неприятность: если хочешь сохранить анонимность, лучше выбрать WebMoney. CyberPlat — это единственная система, где нужно указывать свои реальные данные. Никакой анонимности, все как в банке. С Cyberplat не работают интернет-магазины, они предпочитают WebMoney и «Яндекс.Деньги».

В CyberPlat жестко определены все плательщики (дилеры, которые принимают платежи) и получатели (провайдеры, операторы сотовой связи). Все операции заверяются электронной подписью, которая имеет юридическую силу. Придумать какой-нибудь вариант мошенничества для этой системы довольно сложно. Вывод денег со счета дилера «куда угодно» невозможен. Ди-

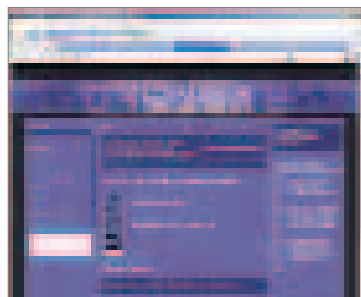


«Яндекс.Деньги»

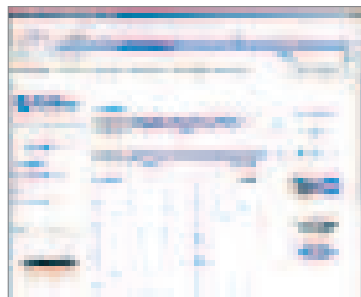


«Рапида»

ЕСЛИ ВАЖЕН ДОСТУП С МОБИЛЬНОГО ТЕЛЕФОНА, ОСТАНОВИ СВОЙ ВЫБОР НА СИСТЕМАХ, ПОДДЕРЖИВАЮЩИХ SMS-ПЛАТЕЖИ

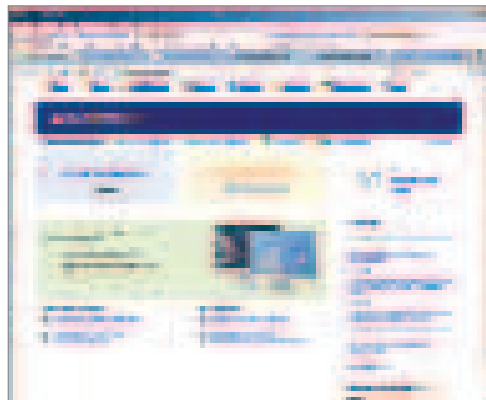


КредитПилот



WebMoney

«Деньги@Mail.ru»



лер имеет право перечислить деньги только на строго определенные счета (провайдеру, оператору и т.д.), после перевода деньги будут зачислены на лицевой счет абонента. Обычно CyberPlat используется для оплаты счетов провайдеров, сотовых операторов, хостинг-провайдеров и т.д.

Ты часто бываешь в пути? Хочешь управлять своим кошельком с мобильного? Хочешь отправлять деньги всего одной SMS'кой? Понимаю тебя: носить ноутбук с собой лень. Если доступ к мобильки важен, рекомендую остановить свой выбор на системах WebMoney, E-port и «Рапида», которые поддерживают SMS-

платежи. Впервые этот сервис осуществила система E-port. Доступ к виртуальной карте E-port можно получить с любого мобильного устройства, поддерживающего WAP.

Хочешь отправить деньги на e-mail? Без проблем. Тогда стоит обратить внимание на «Яндекс.Деньги», она заслуживает отдельного разговора. Система появилась в 2002 году в результате сотрудничества компании «Яндекс» и международной системы PayCash, которая специализируется на платежах в интернете. С самого начала работа в системе напоминала работу с WebMoney: скачать программу, пройти

регистрацию и работать с системой посредством этой программы. Относительно недавно (с октября этого года) ситуация изменилась, теперь для получения доступа к кошельку используется web-интерфейс. Как уверяют в PayCash, с безопасностью у web-интерфейса системы все в порядке, поэтому можешь не волноваться за свои деньги. Но я из соображений этой же безопасности остановил свой выбор на интернет-кошельке. С программой разрешается работать как интернет-магазинам, так и обычным пользователям, которым не нравится web-интерфейс и которые предпочитают интерфейс программы «Интернет-кошелек».

Если ты используешь web-интерфейс, то можешь отправить деньги пользователю на обычный адрес электронной почты. Подробнее об этом на сайте <http://money.yandex.ru>.

Система «Яндекс.Деньги» работает только с рублями, поэтому территория ее возможного использования ограничена.

Для международных платежей лучше выбрать другую систему, поддерживающую доллар или евро. «Яндекс.Деньги» же удобна для оплаты услуг мобильной и стационарной связи, коммунальных услуг, доступа к игровым ресурсам (интернет-казино), покупок в интернет-магазинах.

Тянет к чему-то новому? Система



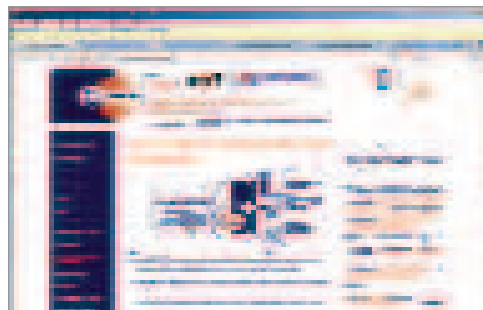
MoneyMail была создана усилиями московского «Мегаватт-банка» в 2004 году. Первоначально система использовалась только для партнерских банков, но с весны 2005 года к ней открыт доступ всем желающим. В конце сентября этого же года был запущен web-интерфейс для этой системы — «Деньги@Mail.ru». Стать клиентом сервиса очень просто: заходишь на сайт и регистрируешься. Ясно (смотри название системы), что клиенты MoneyMail могут посылать деньги прямо на электронные ящики.

CyberPlat

Система MoneyMail позволяет хранить деньги в рублях, долларах и евро. Ее можно использовать для оплаты услуг мобильной/стационарной телефонной связи, коммунальных услуг и погашения кредитов.

Хочешь выбрать универсальную систему и не морочить себе голову? Выбирай WebMoney — ее знают во всем мире, ты можешь платить с ее помощью хоть в США, хоть в Европе. К тому же доступ к твоему WM-кошельку возможен с любой точки земного шара благодаря WM Keeper Light (об этом подробнее — на сайте www.webmoney.ru).

Мы рассмотрели все системы, кроме «Рапиды» и «КредитПилот». Это довольно специфические системы, и пользоваться ими, скорее всего, ты будешь



E-port

редко. «Рапида» была создана в 2001 году усилиями двух банков: «Гута-банка» и «Инком-банка». К разработке приложили руку программисты довольно известных в IT-мире компаний: «АйТи» и «Информзащита». Если ты хочешь заплатить за что-то с помощью «Рапиды», покупай соответствующую предоплаченную карту и, используя ее реквизиты, регистрируйся на сайте www.rapida.ru. После регистрации для тебя будет создан индивидуальный баланс — UserID, идентификатор пользователя, который в дальнейшем используется для входа на сайт. Платежи осуществляются и по интернету, и с мобильного телефона (с помощью SMS). Комиссия небольшая: за перевод другому пользователю «Рапиды» всего лишь 0,5%. Правда, в «Рапиде» есть лимит на разовый платеж — 60 тыс. рублей. Также нужно отметить, что «Рапида» в основном используется в банковском секторе.

Адрес сайта системы «КредитПилот» — www.kreditpilot.ru/html. С ее помощью ты можешь оплачивать услуги связи мобильных и стационарных телефонных операторов, оплачивать интернет и спутниковое ТВ. Но это далеко не все. «КредитПилот» может использоваться и для платежей в интернет-магазинах, никаких ограничений по этому поводу нет.

- пополнить свой счет в «КредитПилот» можно тремя способами:**
- 1 БАНКОВСКИМ ПЛАТЕЖОМ;
 - 2 ПОЧТОВЫМ ПЕРЕВОДОМ;
 - 3 С ПОМОЩЬЮ ПРЕДОПЛАЧЕННОЙ (ПЛАТЕЖНОЙ) КАРТЫ.

Каталог интернет-магазинов, работающих с «КредитПилот», ты найдешь по адресу www.kreditpilot.com/html/shoplist.html — есть все от бытовой техники до цветов и подарков.

Надеюсь, наш краткий экскурс помог тебе выбрать платежную систему или платежные системы (никто не мешает открыть счета сразу во всех платежных системах мира, главное — не запутаться потом) и начать в них хоть немного ориентироваться.

ДЛЯ КАЖДОГО ТЕЛЕВИДЕНИЯ

GO TV VIEW

www.go-tv.ru

GO TV VIEW FOR CRYSTAL

Самый популярный формат в кабельных сетях. Подходит для телевизоров с экраном от 10 до 42 дюймов. Поддерживает все форматы видео и аудио. Высокая контрастность и яркость. Широкий динамический диапазон. Поддержка 3D-форматов.

GO TV VIEW FOR HD

Самый популярный формат в кабельных сетях. Подходит для телевизоров с экраном от 10 до 42 дюймов. Поддерживает все форматы видео и аудио. Высокая контрастность и яркость. Широкий динамический диапазон. Поддержка 3D-форматов.

GO TV VIEW FOR HD

Самый популярный формат в кабельных сетях. Подходит для телевизоров с экраном от 10 до 42 дюймов. Поддерживает все форматы видео и аудио. Высокая контрастность и яркость. Широкий динамический диапазон. Поддержка 3D-форматов.

GO TV VIEW FOR HD

Самый популярный формат в кабельных сетях. Подходит для телевизоров с экраном от 10 до 42 дюймов. Поддерживает все форматы видео и аудио. Высокая контрастность и яркость. Широкий динамический диапазон. Поддержка 3D-форматов.

GO TV VIEW FOR HD

Самый популярный формат в кабельных сетях. Подходит для телевизоров с экраном от 10 до 42 дюймов. Поддерживает все форматы видео и аудио. Высокая контрастность и яркость. Широкий динамический диапазон. Поддержка 3D-форматов.

GO TV VIEW FOR HD

Самый популярный формат в кабельных сетях. Подходит для телевизоров с экраном от 10 до 42 дюймов. Поддерживает все форматы видео и аудио. Высокая контрастность и яркость. Широкий динамический диапазон. Поддержка 3D-форматов.

GO TV VIEW FOR HD

Самый популярный формат в кабельных сетях. Подходит для телевизоров с экраном от 10 до 42 дюймов. Поддерживает все форматы видео и аудио. Высокая контрастность и яркость. Широкий динамический диапазон. Поддержка 3D-форматов.

КТО? ГДЕ? КОГДА?

КОГДА И ПОЧЕМУ УДОБНЕЕ ПРИМЕНЯТЬ ОПРЕДЕЛЕННУЮ ЭЛЕКТРОННУЮ ПЛАТЕЖНУЮ СИСТЕМУ

НИ ДЛЯ КОГО НЕ СЕКРЕТ, ЧТО ВСЕ ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ ПРЕДОСТАВЛЯЮТ СОВЕРШЕННО РАЗНЫЕ ВОЗМОЖНОСТИ. А ТЫ С КАКОЙ ЦЕЛЬЮ ПОЛЬЗУЕШЬСЯ E-MONEY? ПОЭТОМУ ТЫ И ВЫБРАЛ «ИМЕННО ЭТУ» СИСТЕМУ, А НЕ ДРУГУЮ. В ЭТОЙ СТАТЬЕ ОБСУДИМ ДОСТОИНСТВА И УДОБСТВО КАЖДОЙ ИЗ ЧЕТЫРЕХ ОСНОВНЫХ РОССИЙСКИХ ПЛАТЕЖНЫХ СИСТЕМ: WEBMONEY, «ЯНДЕКС.ДЕНЬГИ», CYBERPLAT И E-PORT ^{DHS}

webmoney Эта система может работать с американским долларом (WMZ), евро (WME), рублем (WMR), украинской гривной (WMU) и узбекским сумом. Для нас с тобой актуальнее всего доллар и рубль. Самый простой способ пополнения кошелька — WM-карта. Здесь есть только одно «но»: WM-карточки пока не продаются на каждом углу и их можно найти не по всей стране, что доставляет определенные неудобства. Максимально приемлемый способ — это банковский перевод. Все подробности ты найдешь на сайте Webmoney. Вывод денег также достаточно прост и наиболее удобен через банк или систему Western Union. Можно также обменять WMZ на наличные через специальные пункты, которые есть во многих странах. Обычно комиссия при переводе денег через эти пункты ниже, чем в случае с Western Union. Способов ввода/вывода рубля гораздо больше — это, прежде всего, тот же банковский перевод (можно реализовать и через «Сбербанк»), также с помощью карты, почтовым переводом, наличными в банкоматах, через обменные пункты и даже с помощью SMS. Доллар и рубль — основные расчетные единицы, а о способах снятия других валют ты можешь почитать на сайте Webmoney.

вердикт: СИСТЕМА WEBMONEY ОЧЕНЬ УДОБНА ДЛЯ НЕБОЛЬШИХ ПОКУПОК В ИНТЕРНЕТЕ (АУДИО-ВИДЕОКОНТЕНТ, ЭЛЕКТРОННЫЕ КНИГИ И Т.Д.), ОПЛАТЫ РЕКЛАМЫ (БАННЕРОВ И ПРОЧ.) И ПЕРЕВОДОВ СРЕДСТВ ФРИЛАНСерам.

«ЯНДЕКС.ДЕНЬГИ» Оперировать тоже только рублями, но она универсальнее Cyberplat. Система позволяет внести деньги на свой кошелек, перевести деньги другому абоненту системы, вывести деньги (получить наличные), произвести покупку в интернет-магазине, который работает с «Яндекс.Деньги», заплатить за коммунальные услуги и т.д. Для пополнения же счета существует четыре основных способа. Первый из них — банковский перевод, второй — предоплаченная карточка «Яндекс.Деньги», третий — оплата наличными в офисе компании и, наконец, последний — почтовый перевод. Для вывода всего два способа: оплата наличными в офисе и банковский перевод. «Яндекс.Деньги» работает только с российскими рублями. Тем не менее, благодаря давнему родству системы с PayCash позволены покупки в любых интернет-магазинах, подключенных к иностранным представительствам PayCash, что дает очень широкие возможности.

вердикт: СИСТЕМА «ЯНДЕКС.ДЕНЬГИ» ОЧЕНЬ УДОБНА ДЛЯ ОПЛАТЫ РАЗЛИЧНЫХ ОНЛАЙНОВЫХ ИГР, УСЛУГ ФИКСИРОВАННОЙ И МОБИЛЬНОЙ СВЯЗИ, А ТАКЖЕ ДЛЯ ПОКУПОК В ИНТЕРНЕТ-МАГАЗИНАХ.

e-port Работа с этой системой осуществляется с помощью платежных карт e-port, которые бывают двух видов: физические (действуют только по Москве) и виртуальные. Виртуальные карты невозможно пощупать, но они действуют везде, где есть интернет. Виртуальную платежную карту нулевого номинала можно получить бесплатно — другими словами, зарегистрироваться в системе не стоит нисколько, и потом карта пополняется до нужного номинала. Пополнить платежную карту E-port можно несколькими способами: наличными, с помощью банковского перевода, в офисе компании, с помощью банковских карт (STB). С выводом денежных средств с карты похуже: или в офисе наличными, или безналичным банковским переводом. К достоинствам системы можно отнести возможность проведения платежей с помощью мобильного телефона. Поддерживается также проведение платежей с помощью SMS. Любопытно, что подобная операция доступна даже когда ты находишься в другой стране — роуминг полностью поддерживается. Дилерская сеть E-port хорошо развита и насчитывает на сегодняшний день свыше семи тысяч пунктов приема платежей в 78-ми регионах нашей страны.

вердикт: ПРЕЖДЕ ВСЕГО E-PORT ОЧЕНЬ УДОБНА ДЛЯ ОПЛАТЫ СОТОВОЙ СВЯЗИ И КОММУНАЛЬНЫХ УСЛУГ БЛАГОДАРЯ РАЗВИТОЙ ДИЛЕРСКОЙ СЕТИ, А ТАКЖЕ КАБЕЛЬНОГО И СПУТНИКОВОГО ТЕЛЕВИДЕНИЯ.

cyberplat Несколько специфическая система. В ней ты пополняешь свой счет для оплаты услуг фиксированных провайдеров: поставщиков мобильной и стационарной телефонной связи, интернет-услуг, — плюс оплачиваешь коммунальные услуги. Ты не можешь отправить деньги любому пользователю системы. Система предназначена исключительно для юридических лиц в том смысле, что в ней возможны лишь операции, присутствующие сегментам B2B и B2C. В системе невозможна анонимная регистрация, что существенно повышает ее безопасность для корпоративного сектора. Поскольку система Cyberplat используется только для оплаты услуг в пределах России, она оперирует только рублями и другие валюты не поддерживаются. Принцип работы с системой заключается в следующем: ты пополняешь свой счет в одном из пунктов приема платежей (дилерская сеть Cyberplat довольно разветвленная), потом распоряжаешься находящимися на счету средствами по своему усмотрению — платишь за коммунальные услуги, пополняешь счет у своего интернет-провайдера или баланс мобильного телефона.

вердикт: СИСТЕМА CYBERPLAT ОЧЕНЬ УДОБНА ДЛЯ ОПЛАТЫ КОММУНАЛЬНЫХ УСЛУГ И МОБИЛЬНОЙ СВЯЗИ, УСЛУГ ИНТЕРНЕТ-ПРОВАЙДЕРОВ, КАБЕЛЬНОГО И СПУТНИКОВОГО ТЕЛЕВИДЕНИЯ.



особое мнение

КАКОЕ БУДУЩЕЕ У ЭЛЕКТРОННЫХ ДЕНЕГ

ОЧЕРЕДНОЙ ОПРОС ПО ТЕМЕ НОМЕРА. ОЧЕРЕДНОЕ МНЕНИЕ АВТОРИТЕТОВ :). В ЭТОТ РАЗ ОПРОШЕНЫ И ТЕ, КТО ХОРОШО ИЗВЕСТНЫ ТЕБЕ ПО ПУБЛИКАЦИЯМ В СЕТИ ИЛИ НАШЕМ ЖУРНАЛЕ, И ТЕ, КОГО ТЫ ЕДВА ЛИ ЗНАЕШЬ, НО ИХ ОТВЕТЫ ПОЗНАВАТЕЛЬНЫ. МЫ ПОСТАРАЛИСЬ ЗАДАТЬ СКОЛЬЗКИЕ ВОПРОСЫ, ЧТОБЫ ПОЛУЧИТЬ ИНТЕРЕСНЫЕ ОТВЕТЫ. ВОТ ЧТО ИЗ ЭТОГО ПОЛУЧИЛОСЬ | **АНДРЕЙ КАРОЛИК (WWW.FORCETEAM.RU)**





XS: ЗАМЕНЯТ ЛИ ЭЛЕКТРОННЫЕ ДЕНЬГИ ОБЫЧНЫЕ?

СЕРГЕЙ ПОЛЯНСКИЙ (ROBOX, www.roboxchange.com): Я бы не рассматривал электронные деньги как альтернативу обычным. Электронные, скорее — дополнительная форма существования обычных денег, просто более удобная и специально приспособленная для мгновенных расчетов в интернете.

ЗАРАЗА (IT сайта www.security.nnov.ru): Полностью, разумеется, не заменят. У обычных денег есть свойство анонимности и физической доступности — это и преимущество, и недостаток. Но электронные деньги вполне могут очень сильно потеснить обычные.

Bad_guy (основатель портала исследования защиты программ CRACKLAB, www.cracklab.ru): По-видимому, да, потому как, если учесть всеобщую компьютеризацию, с каждым днем все больше торговых организаций и частных лиц осознанно используют электронные деньги по соображениям удобства. Так что лет через сто каждая бабуса будет покупать себе краюшку хлеба на электронные деньги :).

ДМИТРИЙ СОШНИКОВ (доцент Кафедры вычислительной математики и программирования МАИ, руководитель группы искусственного интеллекта MAILabs, dsh@mailabs.ru): Скорее всего, нет. Если говорить об электронных платежах типа WebMoney, то ответ однозначен. Если же речь идет о «пластиковых деньгах», безналичных расчетах и т.д., то уже сейчас перевес существует в пользу последних. Люди все больше доверяют пластику и понимают удобство расчетов такого рода. Однако даже в США, где без кредитки прожить сложно, больше половины расчетов в супермаркетах, киосках и т.д. производится наличными.

АЛЕКСЕЙ ЛУКАЦКИЙ (Cisco Systems): Если и заменят, то мы будем ждать этого очень долго. Потребуется не только изменение многих бизнес-процессов, но и информатизация отдаленных уголков всей планеты. В романе Тобиаса Хилла «Криптограф» замечательно описано это будущее. При этом надо понимать, что замена обычных денежных и, тем более, товарных отношений на электронные финансы потребует немалых вложений и в информатизацию общества, в его обучение, и на то, чтобы общество доверяло электронным деньгам так же, как и зеленым бумажкам.

КРИС КАСПЕРСКИ (Мыцдх, <ftp://nezumi.org.ru>): Электронные деньги в настоящий момент занимают лишь малую часть общего оборота, они игнорируются правительством и банками, к тому же единого стандарта на электронную наличность нет и существует куча платежных систем, каждая из которых имеет огромное количество проблем (прежде всего с безопасностью). Такая постановка вопроса вопиюще некорректна. «Бумажных денег» на Западе давно нет. Если поднять психологические тесты, то во многих из них можно встретить вопрос: «Предпочитаете ли вы «кэш» (наличность) остальным системам оплаты (кредиткам, чекам)?» Человек, любящий хрустящие купюры, считается не вполне адекватным социальным типом :). Между тем, гибель бумажных денег на Западе еще не означает торжество электронных...

XS: ПОЧЕМУ ИЗ ВСЕХ ПЛАТЕЖНЫХ СИСТЕМ НАИБОЛЬШЕЕ РАСПРОСТРАНЕНИЕ ПОЛУЧИЛА WEBMONEY, ХОТЯ ПРИНЦИП РАБОТЫ У ВСЕХ СИСТЕМ АНАЛОГИЧНЫЙ.

СЕРГЕЙ ПОЛЯНСКИЙ: Просто потому что WebMoney была первой — это огромное конкурентное преимущество, с которым очень трудно бороться. Выход каждого следующего конкурента на близкий уровень к лидеру рынка дается лишь с затратами на порядок больше. Малевич, который первым нарисовал «Черный квадрат», прославился на весь мир. У его последователей, рисовавших «синие треугольники» и «красные круги», видимо, не хватило ресурсов для раскрутки своих творений. Шутка, конечно, но общий смысл в этом. Тот, кто первым реализовал оригинальную идею, снимает сливки с рынка.

ЗАРАЗА: Рынок развивался по принципу снежного кома. Если кто-то один раз вырвался вперед, он и получит самые большие накрутки в дальнейшем. Остальным придется добирать то, что осталось.

BAD_GUY: Возможно, это и громко сказано. За рубежом весьма популярны Neteller и e-gold, у них многие ничего не слышали о WebMoney, а у нас это наиболее развитая система. Тот, кто захочет платить мне электронными деньгами, воспользуется именно WebMoney, потому как для меня потом будет проще пристроить их куда-либо, заплатив меньшую комиссию. Пожалуй, единственная система, которая, кроме WebMoney, как-то может претендовать на удобство, — это «Яндекс.Деньги». Правда, на этой системе меньше вариантов что-то куда-то перевести, купить что-то на «Яндекс.Деньги» тоже сложнее. Комиссия же взимается не с отправителя, а с получателя перевода, что очень неудобно и заставляет продавца открыто повышать цену товара на эту комиссию — для покупателя это выглядит не как комиссия системы, а как цена товара, менее выгодная по сравнению с предложениями других продавцов.

ДМИТРИЙ СОШНИКОВ: Наверное, тут сказывается своевременность выхода на рынок. WebMoney были первой крупной и получившей распространение системой — в финансовом секторе многое строится на доверии, поэтому системы, которые просуществовали долго и имеют большой оборот, автоматически получают повышенный приток новых пользователей. Срабатывает эффект «снежного кома».

АЛЕКСЕЙ ЛУКАЦКИЙ: Как давно известно из теории маркетинга, выигрывает не тот, у кого технологии лучше, а тот, кто больше рекламируется. Немного утрировано, но суть именно такая. Главное — уметь подать свой товар и заинтересовать им потребителя, а потом уже сам клиент доведет начатое до конца, распространив знание о «замечательной» технологии по всем своим знакомым (так называемый «эффект лавины»). WebMoney воспользовались этим гораздо грамотнее своих конкурентов.

КРИС КАСПЕРСКИ: Принцип работы у других систем совсем не аналогичный! Можно насчитать свыше десяти различных схем. И схема, используемая WebMoney — это типичная пирамида, которая идеально подходит для того, чтобы в один прекрасный момент WebMoney могла беспрепятственно завладеть всем капиталом, оставаясь юридически чистой. Я не говорю, что она сделает это или собирается, но то, что сама схема оптимизирована под построение пирамиды, факт. Почему она стала популярной? Так ведь пирамида :). К тому же реклама, пропаганда и т.д.

XS: НЕПОЯТНО, ЧЕМ ОБЕСПЕЧЕНА БОЛЬШАЯ ЧАСТЬ УСЛОВНЫХ СРЕДСТВ (ЭЛЕКТРОННЫЕ ДЕНЬГИ) В СИСТЕМЕ WEBMONEY. ПРОСТОМУ ПОЛЬЗОВАТЕЛЮ НЕИЗВЕСТНА, И ДЛЯ НЕГО НЕПРОЗРАЧНА СИСТЕМА УЧЕТА ДВИЖЕНИЯ ПОТОКОВ ВНУТРИ СИСТЕМЫ WEBMONEY. КАЖЕТСЯ, ЧТО ВСЕ РАБОТАЕТ ТОЛЬКО ПОТОМУ ЧТО ЕСТЬ ПРИТОК НОВЫХ ПОЛЬЗОВАТЕЛЕЙ...

СЕРГЕЙ ПОЛЯНСКИЙ: Конечно же, WebMoney живет НЕ за счет притока новых пользователей, а за счет оборота своих электронных денег. Посмотри на статистику WebMoney, умножь эту цифру на комиссию системы и поймешь. Платежные системы имеют два основных источника дохода: комиссия за перевод электронных денег и скидки продавцов (то есть тех поставщиков товаров и услуг, которые принимают эти деньги). Оборот электронных денег по большому счету имеет только одно направление: их вводят в обращение конечные пользователи, и деньги оседают на электронных счетах поставщиков товаров и услуг, которые, в свою очередь, гасят эти средства у эмитента, получая взамен обычные деньги на безналичный счет. Как только платежная система перестанет отвечать по этим обязательствам — все, считай, она банкрот. Так как информация в Сети распространяется очень быстро, эту ответственность можно считать еще более тяжелой. Именно этот факт заставляет платежные системы держать обеспечение под свои электронные деньги, и я думаю, что размер этого обеспечения существенно больше, чем, например, в банковской сфере. Именно за счет того, что динамика выше и цена ошибки выше. Так что можно считать, что электронные деньги как форма существования денег в какой-то мере лучше чем, например, банковский депозит (только нет процентов по вкладам).

ЗАРАЗА



РЕДАКТОР САЙТА
www.security.nnov.ru,
ЖИВЕТ И РАБОТАЕТ
В НИЖНЕМ НОВГОРОДЕ.
СФЕРА ДЕЯТЕЛЬНОСТИ —
ТЕЛЕКОММУНИКАЦИИ.
ХОББИ — ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ И УЯЗВИМОСТИ
ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

ЗАРАЗА: Ну, это как раз чушь. Причем тут приток новых пользователей? WebMoney существует за

счет достаточно высокого процента с транзакций и за счет получения прибыли с уже имеющихся оборотных средств (тебе же никто не платит процент за то, что ты держишь свои деньги в WebMoney). И доход этот совсем не маленький, так что для WebMoney, в отличие от той же пирамиды, экономически нецелесообразно рушиться. Если рассматривать аккаунт WebMoney как банковский счет, а не как ценные бумаги, то вопрос обеспечения можно задать любому коммерческому банку. Банку невыгодно обеспечивать чем-либо твои вклады, ему выгодней самому вкладывать их. Вот вопрос отсутствия финансового контроля — это да.

BAD_GUY: WebMoney не обещает нам по 2000% годовых, то есть WebMoney — явно не «МММ». Система WebMoney живет на комиссии с переводов. Однако держать в системе солидные суммы и «копить себе на пенсию» я бы не стал. И вообще в нашей стране можно доверять только драгметаллам и недвижимости.

ДМИТРИЙ СОШНИКОВ: Электронные деньги WebMoney обеспечены реальными деньгами, которые в них вкладывают участники системы, по крайней мере, в первом приближении. А вообще ситуация такая же, как с банками, которые тоже лопнут, если все вкладчики побегут забирать деньги. В этом смысле WebMoney даже лучше: мало кто хранит в них значительные сбережения. Так что банки как институт пока живы, и такое же право на жизнь имеют электронные деньги.

АЛЕКСЕЙ ЛУКАЦКИЙ: Мне трудно говорить об обеспечении WebMoney, я не знаком с их финансовыми документами.

КРИС КАСПЕРСКИ: Не совсем. WebMoney продает электронные единицы за ЖИВЫЕ деньги, то есть попросту торгует воздухом, при этом не стесняясь брать комиссию за перевод. В очень грубом приближении WebMoney — это банк, а электронный кошелек — это чек. Банк живет за счет того, что крутит деньги. Только банк ГАРАНТИРУЕТ возврат денег, а WebMoney лишь сохраняет за тобой «имущественные права». Выкуп же электронных денег «гарантируют» гаранты, с которыми ты не заключал никакого договора и у которых твоих денег нет. Похоже на то, как в стране создается предположение к инфляции всякий раз, когда государство включает печатный станок. А теперь представь, что произойдет, если этот печатный станок окажется у компании, которая даже не желает нанять пару голодных студентов для создания круглосуточной службы поддержки.

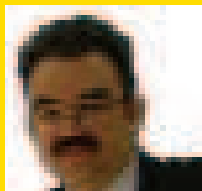
XS: ЗЛЫЕ ЯЗЫКИ УТВЕРЖДАЮТ, ЧТО СИСТЕМА WEBMONEY НЕ ИМЕЕТ ЮРИДИЧЕСКОГО СТАТУСА. ПОЧЕМУ ЖЕ ПОЛЬЗОВАТЕЛИ ДОВЕРЯЮТ WEBMONEY?

СЕРГЕЙ ПОЛЯНСКИЙ: На тему юридического статуса ничего нового не скажу. Поскольку эта тема не имеет, в силу своей новизны, юридического приземления, каждый пытается найти какие-то аналоги, так или иначе отражающие суть электронных денег. Вот и все. Может быть, юридическое «приземление» электронных денег от WebMoney и не самое удачное, а может, наоборот — рассудит время.

ЗАРАЗА: Возможно, доверяют из-за безвыходности. В данном случае придется искать компромисс между удобством и риском. Но держать крупную сумму (порядка нескольких тысяч долларов) в электронном кошельке даже на короткий промежуток времени я бы не стал. И вообще я постарался бы избежать передачи таких сумм через любую «не банковскую» систему, пусть даже я потерял бы более высокий процент. По тем же самым причинам я не стал бы хранить дома или носить с собой крупную сумму наличных.

BAD_GUY: Мне нравится одна мысль, которую я для себя вынес после общения с букмекерскими конторами. Вся наша жизнь представляет собой

**АЛЕКСЕЙ
ЛУКАЦКИЙ**



СЕЙЧАС РАБОТАЕТ В CISCO И ОТВЕЧАЕТ ЗА РАЗВИТИЕ НАПРАВЛЕНИЯ SECURITY НА ТЕРРИТОРИИ РОССИИ И СТРАН СНГ. А НАЧИНАЛ ДОСТАТОЧНО ТРАДИЦИОННО — ПРОГРАММИРОВАЛ КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ НА АССЕМБЛЕРЕ В ОДНОМ ИЗ МОСКОВСКИХ «ЯЩИКОВ». ПОТОМ ПУТЬ ЛЕЖАЛ ОТ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ К АНАЛИТИКУ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ. СЕЙЧАС НЕМНОГО УШЕЛ ОТ «ТЕХНИКИ» И ЗАНИМАЕТСЯ УСТРАНИЕНИЕМ ИНТЕРВАЛА МЕЖДУ ТЕХНИЧЕСКОЙ СТОРОНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ БИЗНЕС-СОСТАВЛЯЮЩЕЙ

КРИС КАСПЕРСКИ

ЗАТВОРНЫЙ МЫЩЬХ, ЖИВУЩИЙ В ГЛУБИНЕ ПЕЩЕРЫ СВОЕГО СОЗНАНИЯ. А НОРА, КАК ИЗВЕСТНО, — ЭТО ДЫРА (В БЕЗОПАСНОСТИ). ЗДЕСЬ ВОДЯТСЯ ОТЛАДЧИКИ, ДИЗАССЕМБЛЕРЫ И ЕЩЕ ТРИ ТЕЛЕСКОПА, В КОТОРЫЕ ОН СМОТРИТ НА НЕБО, КОГДА НИЧЕГО НЕ ХОЧЕТ

риск, все наши финансовые операции тоже представляют собой риск. Поэтому, прикинув вероятности, можно временно доверить WebMoney пару сотен баксов. И ничего страшного, если в конце концов даже такая сумма потеряется — просто вероятность этого очень мала и, скорее всего, все будет успешно.

ДМИТРИЙ СОШНИКОВ: В некотором смысле, так происходит из-за несовершенства банковских институтов. Пользуясь WebMoney, мы платим меньший процент за перевод денег, но при этом рискуем больше, так как нет аналогов закона о защите вкладов государством. Однако в конечном счете электронные деньги можно просто рассматривать как удобный способ обмена наличностью — в этом случае риск не так велик и локализован по времени.

АЛЕКСЕЙ ЛУКАЦКИЙ: В лицензиях на платное программное обеспечение всегда имеется фраза наподобие «оно продается "как есть"», и разработчик не несет никаких гарантий». Когда мы въезжаем в новую квартиру, ситуация аналогична: если дом рухнет, то предъявлять претензии можно сколько угодно долго без ясного результата, достаточно вспомнить ситуацию с «Трансвааль-парком». Опять же, если системе доверяют, то ее юридический статус не так важен. Если не доверяют, то даже куча юридически грамотных документов ничего не решит.

КРИС КАСПЕРСКИ: WebMoney доверяют далеко не все, причем доверяют только в надежде на авось. Количество пострадавших или обиженных просто огромно. Форумы буквально ломятся от сообщений на эту тему. Так что говорить о «доверии» в такой ситуации несколько странно.

XS: ПЛАТЕЖНЫЕ СИСТЕМЫ УТВЕРЖДАЮТ, ЧТО ВЗЛОМАТЬ ИХ ПРАКТИЧЕСКИ НЕВОЗМОЖНО. ХАКЕРЫ ГОВОРЯТ ОБ ОБРАТНОМ. ЧТО ЖЕ НА САМОМ ДЕЛЕ?

СЕРГЕЙ ПОЛЯНСКИЙ: На самом деле взломать можно ВСЕ — дело лишь в вопросе экономической целесообразности. Никто не станет ломать сейф и тратить на эту операцию \$1000, если известно, что в этом сейфе вряд ли хранится больше, чем десять тысяч рублей. Взлом самой платежной системы, по большому счету, просто лишен смысла, потому что, в отличие от банковского хранилища, где хранятся деньги (которые, как известно, не пахнут), там не хранится никаких материальных ценностей, которые можно «унести и спрятать». Кроме того, операции мошенников для эмитента электронных денег обратимы: основным объектом нападков являются кошельки пользователей.

ЗАРАЗА: На самом деле каждый комментирует защищенность со своих позиций. Если кто-то увел твой кошелек WebMoney через троянец на твоей машине, кого взломали? WebMoney или тебя? WebMoney скажет, что тебя. Кто-то может сказать, что взломали WebMoney. Вопрос упирается в определение того, что является платежной системой и на чем она заканчивается. Является ли ПО для работы с кошельком и компьютер пользователя частью платежной системы? По-моему, да. Взломать можно все, но ломать-то будут в самом уязвимом месте.

BAD_GUY: Допустим, есть хакер, который знает, как воровать деньги, например, из системы e-gold. Естественно, это его «хлеб», и об этом хакер не расскажет даже ближайшему другу. Значит, общественность не узнает о факте уязвимости в системе. Возможно, если суммы краж хакера будут мелкими для системы в целом, то хищение даже не заметят, разбираться не будут. Но если пойдет речь о сотнях долларов, заметят и проведут расследование, соответственно, рано или поздно будут найдены следы вывода средств, которые в принципе могут привести к хакеру, и тот будет тихо обезврежен, а о его деяниях общественность, опять же, не узнает. Системе невыгодно, чтобы ей перестали доверять толпы многочисленных клиентов.

АЛЕКСЕЙ ЛУКАЦКИЙ: Правы обе стороны, каждый судит со своих позиций. Платежная система не может говорить, что она уязвима, иначе потребитель от нее отвернется. Кроме того, когда платежная система заявляет о своей уязвимости, то речь идет, как правило, о математической стороне вопроса, то есть о криптографии. Однако платежная система — это еще и реализация криптографии, и другие программные компоненты, и организационные вопросы, и люди. Слабость в каждом из этих элементов сказывается на системе в целом. И, конечно же, надо помнить о золотом правиле безопасности — «100% безопасности не существует».

КРИС КАСПЕРСКИ: Смотри что понимать под «взломом». Создать генератор электронных единиц WebMoney действительно невозможно. Проникнуть на центральный сервер в принципе, возможно, поскольку ВСЕ реализации стека TCP/IP не свободны от дыр. Даже если там будет использоваться своя собственная ось, 100% гарантии надежности нет. Но такой взлом — довольно сложное дело. Если админ не лось, взлом крайне маловероятен. Однако последствия взлома губительны, и полностью списывать его со счетов нельзя. В настоящее время хакеры занима-

ются тем, что воруют электронные кошельки. Это не взлом самой платежной системы — это просто воровство, но оно процветает...

XS: ИЛИ ЖЕ В ОСНОВНОМ КРАЖИ ЭЛЕКТРОННОЙ НАЛИЧНОСТИ ПРОИСХОДИТ ДЕЙСТВИТЕЛЬНО ИЗ-ЗА «КРИВЫХ РУК»?

СЕРГЕЙ ПОЛЯНСКИЙ: Самая уязвимая часть платежных систем — кошельки пользователей. Думаю, найдется мало людей, у которых хоть раз что-нибудь да не украли — кошелек из сумочки, барсетку с сидения машины и т.п. Почему-то мы все учимся только на своих ошибках. Положи портмоне в задний карман джинсов и походи пару часов в оживленном месте — 90 шансов из 100, что ты лишишься бумажника и не заметишь, как это произошло.

ЗАРАЗА: Есть распространенное мнение, что во взломе своего компьютера всегда виноват пользователь. Пользователь хочет работать с компьютером как с бытовым прибором — холодильником, пылесосом, стиральной машиной — ни о чем не задумываясь и следуя указаниям на экране техники. Чьи кривые руки виноваты в том, что современная индустрия не может ему это обеспечить?

BAD_GUY: Недавно мне начал приходить спам на английском языке. Письма выглядели очень прилично и были присланы якобы от саппорта PayPal. В письме сообщение о том, что с моим аккаунтом (которого у меня в этой системе и вовсе нет) проблемы. Предлагалось кликнуть по ссылке, якобы ведущей на сайт PayPal, но на самом деле она вела на «левый» скрипт на «левом» сайте, который, по-видимому, был призван воровать данные аккаунта владельцев счета PayPal. Кто-то на это попался, но виновата ли одна кривизна рук? Неизвестно. Всегда надо помнить, что обычно крупные системы и сайты никогда ничего не рассылают. А если и пришло незапрашиваемое письмо, не грех спросить по указанному e-mail отправителя, он ли на самом деле послал письмо.

АЛЕКСЕЙ ЛУКАЦКИЙ: Это основная проблема в безопасности. Систему ломают не из-за слабостей в математике, а из-за слабостей в ее реализации. Достаточно допустить ошибку в программировании криптографического алгоритма, и весь его потенциал идет «коту под хвост». Или еще одна распространенная ситуация: программист скачал в интернете исходники криптографической библиотеки и решил, что может создать свою платежную систему, забыв принципы обращения с этой библиотекой. Например, распространенная ошибка — хранение закрытых ключей шифрования в виде незащищенного файла на диске. Стоит злоумышленнику получить доступ к файлу, как вся защищенность платежной системы становится равной нулю. Аналогичная проблема и в администрировании платежных систем. Года три-четыре назад администраторы Western Union проводили регламентные работы на сайте, а по их завершению забыли вернуть все в защищенное состояние. Результат — база клиентов Western Union утекла в интернет.

КРИС КАСПЕРСКИ: Аппаратное обеспечение наших дней не позволяет создать надежный электронный кошелек. В идеале это должно быть отдельное устройство, подключаемое к интернету или поддерживающее работу по протоколам сотовой связи, причем достаточно простое, чтобы вероятность наличия дыр в нем была минимальна. Но таких устройств пока нет, их цена будет слишком высокой, и любой человек скорее воспользуется кредиткой, чем купит соответствующий девайс.

XS: А ВОЗМОЖНО ЛИ ОБЕЗОПАСИТЬ ТО, ЧТО ЗАВЕДОМО РАБОТАЕТ ЧЕРЕЗ «ДЫРЯВЫЕ» ОПЕРАЦИОННЫЕ СИСТЕМЫ И «ДЫРЯВЫЕ» БРАУЗЕРЫ?

СЕРГЕЙ ПОЛЯНСКИЙ: Да, возможно. Читай инструкцию по технике безопасности, прежде чем начать орудовать бензопилой, а не после того,

как ты отпилил себе палец (из собственного опыта). Попробуй поспрашивать пользователей той же WebMoney. Готов спорить, что о существовании подсайта security.webmoney.ru знают не более 10% пользователей WebMoney. Из них прочитали и предприняли рекомендованные меры также не более 10%.

ЗАРАЗА: Нет, нельзя.

BAD_GUY: Конечно, можно ввести ограничения на системные требования и потерять малую долю клиентов, которые пользуются «старьем», чтобы избежать более серьезных проблем. Так и делает, например, WebMoney: «Установив нашу последнюю программу, — говорят они, — чтобы она запустилась на твоём компьютере, или используй IE с SSL версии не ниже такой-то, иначе не станешь нашим клиентом».

АЛЕКСЕЙ ЛУКАЦКИЙ: Это классическая проблема безопасности, которая на сегодня не решаема. Мы либо начинаем повсеместно применять «доверенные» операционные системы, которые хорошо защищены, но абсолютно несовместимы с понятием «удобство использования», либо пользуемся тем, что есть.

BAD_GUY

«BAD_GUY» — ЭТО МОЕ ВТОРОЕ «Я». ПОЧТИ НИКТО ИЗ РЕАЛЬНЫХ ДРУЗЕЙ НЕ ЗНАЕТ, ЧТО Я — ЭТО BAD_GUY. И ПОЧТИ НИКТО ИЗ ИНТЕРНЕТА НЕ ЗНАЕТ, КТО СКРЫВАЕТСЯ ПОД НИКОМ BAD_GUY. КТО-ТО НАЗОВЕТ ЭТО РАЗДВОЕНИЕМ ЛИЧНОСТИ. НО РАЗВЕ ПЛОХО ЖИТЬ ДВЕ ЖИЗНИ СРАЗУ?!»

КРИС КАСПЕРСКИ: Да, такие алгоритмы существуют. Да, можно работать и в заведомо дырявой и агрессивной среде, но... Для этого нужно взять популярную книжку по крипто и почитать ее по диагонали. Разработчики WebMoney до этого еще «не доросли» или умышленно спроектировали систему так, чтобы она была уязвима.

XS: В ЧЕМ ОСНОВНОЕ ПРЕИМУЩЕСТВО ЭЛЕКТРОННЫХ ДЕНЕГ?

СЕРГЕЙ ПОЛЯНСКИЙ: Мгновенные и безопасные расчеты.

ЗАРАЗА: Моментальное осуществление платежа из практически любого места, что позволяет платить в онлайн. Анонимность. Невысокий процент за осуществление перевода для небольших сумм.

BAD_GUY: Моментальные переводы на любые расстояния. Зачастую интересующие тебя люди и их услуги находятся очень далеко от твоего места жительства, а электронные деньги начисто ломают территориальные преграды.

ДМИТРИЙ СОШНИКОВ: Это один из немногих простых и доступных каждому способов организации приема платежей через интернет.

АЛЕКСЕЙ ЛУКАЦКИЙ: Их электронная форма. Мне не надо таскать с собой пачку купюр. Достаточно держать свой кошелек на eToken'e, и я могу расплачиваться за услуги и товары в любом месте, если есть подключение к интернету.

КРИС КАСПЕРСКИ: То, что они не облагаются налогом и позволяют производить анонимные переводы, что делает их привлекательными для жуликов и махинаторов. Я не вижу никаких причин, препятствующих использованию остальных систем оплаты. В частности, мне, чтобы воспользоваться электронными деньгами, придется совершить очень много телодвижений, намного больше, чем даже при банковском переводе. Не говоря уже про кредитки или «Рапиду», которой я пользуюсь чаще всего...

XS: В ЧЕМ ОСНОВНОЙ НЕДОСТАТОК ЭЛЕКТРОННЫХ ДЕНЕГ?

СЕРГЕЙ ПОЛЯНСКИЙ: Отсутствие юридической базы.

ЗАРАЗА: Отсутствие юридической базы. Анонимность. Высокий процент для больших сумм. Да и вообще высокий процент, если учесть, что все платежи идут в рамках одной платежной системы. Низкая безопасность платежной системы. Небольшая сфера применения электронных денег: я все равно должен держать наличные или банковский счет либо и то, и другое. Сложность ввода и вывода денег.

BAD_GUY: Недостаточная распространенность. Например, теми же WebMoney могут беспрепятственно воспользоваться только жители Москвы, Санкт-Петербурга и Новосибирска. С остальными городами, а уж тем более с сельской местностью все намного сложнее: обменников мало, через «Сбербанк» пополнять и выводить средства весьма муторно, да и толпа других мелких сложностей и ограничений, которые отбивают у множества потенциальных клиентов желание стать настоящими клиентами системы.

ДМИТРИЙ СОШНИКОВ: Сложность конвертации в наличные деньги, неликвидность. Если надо заплатить \$10 за доменное имя раз в год, проще воспользоваться кредитной картой, а не заводить электронный кошелек.

АЛЕКСЕЙ ЛУКАЦКИЙ: Их электронная форма. Эти деньги украсть легче, чем обычные банкноты. И с доверием к этим системам пока не все в порядке.

КРИС КАСПЕРСКИ: Если говорить о WebMoney, то она слишком замороженная. Ввод/вывод денег из системы крайне непродуман и неудобен. Если бы он требовал меньше телодвижений, я бы, возможно, и пользовался бы WebMoney для оплаты мелких услуг и заказов.

XS: МОГУТ ЛИ ЭЛЕКТРОННЫЕ ДЕНЬГИ СТАТЬ ЗАМЕНОЙ МИКРОПЛАТЕЖАМ ЧЕРЕЗ СОТОВЫЕ ТЕЛЕФОНЫ?

СЕРГЕЙ ПОЛЯНСКИЙ: Безусловно. И станут. Точнее, вытеснят. Зачем нужен сотовый телефон при платежах в интернете? Просто в настоящий момент это чуть ли единственный счет, на котором практически у каждого человека есть хоть немного денег, а стоимость таких платежей очень высока. Когда люди привыкнут к тому, что пополнять

надо не только свой телефонный счет, но и, например, свой счет «электронных денег», так и будет. Место сотового телефона при проведении платежей через системы электронных денег я вижу, например, в дополнительной идентификации пользователя — в этом я пока не вижу альтернативы им.

ЗАРАЗА: Тут на самом деле возникает сразу два «vs.»: телефон vs. компьютер и электронный счет в банке vs. электронный кошелек. То, что со временем банки должны прийти на рынок онлайн-платежей, однозначно (очень уж жирный кусок), и для этого требуется лишь обеспечить универсальный интерфейс по выставлению и мгновенной оплате счетов. Если бы монстр типа Citigroup вдруг решил сделать это, сразу же появились бы кнопки в интернет-магазинах «оплатить со счета в Ситибанк». Вопрос же безопасности телефона в сравнении с компьютером... Ну, будет у тебя через пять лет на телефоне Windows или что-то выросшее из Symbian OS. Причем с 25% вероятностью это будет PDA-телефон и в стандартной поставке с Internet-мессенджером и NetMeeting для халявного видеотрепа по цене GRPS+Internet, со шлюзом на домашнем компьютере или у сотового оператора. И каким местом станет безопасность телефона? Сразу возникает другой вопрос: «А что надежней: физическая безопасность тебя и сотового телефона или электронная и физическая безопасность домашнего компьютера с электронным кошельком?»

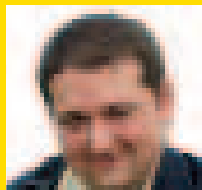
BAD_GUY: Не думаю, что нужно заменять что-то чем-то, оба эти направления платежей весьма перспективны, скорее, надо всячески объединять их и упрощать совместимость. Например, было бы отлично, если бы WebMoney-счет был един со счетом на мобильном телефоне, как и со счетом в банке. Это был бы идеальный вариант, и в конце концов финансовые организации договорятся. Так оно и будет, потому что это удобнее нам — клиентам, а желание клиента — закон. И кто не хочет признавать этого, рано или поздно проиграет.

ДМИТРИЙ СОШНИКОВ: У этих видов платежей разные целевые аудитории, поэтому, скорее всего, они будут долго и мирно сосуществовать...

АЛЕКСЕЙ ЛУКАЦКИЙ: А что такое микроплатежи, как не электронные деньги? Схема такая же, только система называется немного иначе.

КРИС КАСПЕРСКИ: Может быть... Все зависит от того, удастся ли подобрать удачную платежную схему.

**ДМИТРИЙ
СОШНИКОВ**



ДОЦЕНТ КАФЕДРЫ
ВЫЧИСЛИТЕЛЬНОЙ
МАТЕМАТИКИ И
ПРОГРАММИРОВА-
НИЯ МАИ, РУКОВО-
ДИТЕЛЬ ГРУППЫ
ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА MAI-
LABS, dsh@mailabs.ru



электронные обменники

ДЛЯ ЗАЧИСЛЕНИЯ ДЕНЕГ ИЗ ОДНИХ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ В ДРУГИЕ ИСПОЛЗУЮТСЯ ЭЛЕКТРОННЫЕ ОБМЕННИКИ. У КАЖДОГО ИЗ НИХ СВОИ ТАРИФЫ. ПОЛЬЗОВАТЬСЯ ОБМЕННИКОМ ОЧЕНЬ ПРОСТО. ЗАХОДИШЬ НА САЙТ, ВЫБИРАЕШЬ ТУ ВАЛЮТУ, КОТОРАЯ У ТЕБЯ ЕСТЬ, ЗАТЕМ ТУ ВАЛЮТУ, КОТОРУЮ ХОЧЕШЬ ПОЛУЧИТЬ. ПРИ ВЫБОРЕ ВАЛЮТЫ ОБРАТИ ВНИМАНИЕ НА ЕЕ ОСТАТОК НА СЧЕТУ ОБМЕННИКА — ОН УКАЗЫВАЕТСЯ РЯДОМ С НАИМЕНОВАНИЕМ ВАЛЮТЫ. КОНЕЧНО ЖЕ, ЕСЛИ ДЕНЕГ НЕТ, ТО НИКТО НИЧЕГО НЕ ОБМЕНЯЕТ.

ДЕНЬГИ для эксперта

РУКОВОДСТВО ПО ПЛАТЕЖНЫМ ИНТЕРНЕТ-СИСТЕМАМ для опытного пользователя

В ЭТОЙ СТАТЬЕ МЫ ПОГОВОРИМ О ТАРИФАХ ПОПУЛЯРНЫХ ПЛАТЕЖНЫХ СИСТЕМ — WEBMONEY И «ЯНДЕКС.ДЕНЬГИ». ЕСЛИ У ТЕБЯ ЕСТЬ КОММЕРЧЕСКАЯ ЖИЛКА ИЛИ ХОТЯ БЫ ТЫ УМЕЕШЬ СЧИТАТЬ, ТО СЕЙЧАС ПОИМЕШЬ, НАСКОЛЬКО ВЫГОДНЫ ЭЛЕКТРОННЫЕ ДЕНЬГИ. РАДИ ИНТЕРЕСА МОЖЕШЬ ПОЙТИ В БАНК И СРАВНИТЬ ТАРИФЫ НА АНАЛОГИЧНЫЕ БАНКОВСКИЕ ОПЕРАЦИИ ^{DHS}

Начнем, как обычно, с WebMoney. Система не взимает комиссии за ввод средств (то есть ввод средств бесплатен), ты платишь только за услуги той организации, которая переводит деньги (банк, почтовое отделение). Говорить о вводе много не стоит, комиссию банка ты узнаешь, когда придешь в банк. Могу дать только несколько советов.

Никогда не переводи деньги через Сбербанк — обойдется в 5% от суммы перевода. При переводе через почтовое отделение (нужно пользоваться

только электронным) платишь 4%. Но в Сбербанке перевод «идет» три-семь рабочих дней, перевод почтой — один. Выгоднее всего перевод через «Импекс-банк»: всего лишь 2,5% от суммы, время денег «в пути» 15-30 минут. Пока ты дойдешь домой, деньги уже окажутся в твоем кошельке. Зачисление с помощью WM-карты осуществляется мгновенно, но ее еще нужно где-то купить! Не исключено, что в твоем городе не окажется пунктов продажи WM-карт, но в любом случае лучше пойти в «Импекс-банк» — если и добираться

ближе, то особенно порадуешься низкому проценту (при зачислении через WM-карту комиссия продавца карты обычно составляет 5%).

немного подытожим:

1 ЕСЛИ РЯДОМ ЕСТЬ «ИМПЕКС-БАНК», ОБРАЩАЙСЯ ТУДА (2,5%, ВРЕМЯ ЗАЧИСЛЕНИЯ 15-30 МИНУТ).

2 ЕСЛИ РЯДОМ НЕТ «ИМПЕКС-БАНКА», ОБРАЩАЙСЯ НА ПОЧТУ (4%, 1 ДЕНЬ).

3 ЕСЛИ НУЖНО ЗАЧИСЛИТЬ ДЕНЬГИ БЫСТРО, ПОПРОБУЙ НАЙТИ WM-КАРТУ. ЧТОБЫ ТЫ НЕ ИСКАЛ ИХ ДАРОМ, УЗНАЙ НА САЙТЕ www.webmoney.ru, В КАКИХ ГОРОДАХ ОТКРЫТЫ ПУНКТЫ ПРОДАЖИ WM-КАРТ.

4 ЕСЛИ ПОБЛИЗОСТИ ЕСТЬ КОММЕРЧЕСКИЙ БАНК, МОЖНО ПОЙТИ ТУДА: ОБЫЧНО ПЕРЕВОД «ИДЕТ» ОДИН-ДВА ДНЯ, А РАЗМЕР КОМИССИИ УЗНАЕШЬ НА МЕСТЕ, И, СКОРЕЕ ВСЕГО, ОНА НЕ ПРЕВЫСИТ 5-7%.

5 САМОЕ ПОСЛЕДНЕЕ МЕСТО, КУДА ТЫ МОЖЕШЬ ПОЙТИ, — ЭТО ИЗВЕСТНЫЙ ВСЕМ СБЕРБАНК, НО ТЫ УЖЕ ЗНАЕШЬ, ПОЧЕМУ ЭТО МЕСТО «ПОСЛЕДНЕЕ».

Если ни один из этих способов не устраивает тебя, найди информацию о дополнительных путях на www.webmoney.ru. Уверен на все 100%, что ты найдешь то, что устроит тебя.

Теперь перейдем к выводу денег из системы. В таблице подробно описаны тарифы вывода доллара, евро, рубля и гривны.

Проанализируем табличку. Конечно же, в нее включены далеко не все способы вывода денег из системы. Выгоднее всего банковский перевод, но не всегда, так как для его осуществления нужно иметь счет в банке. Western Union пока дороговат, но если нужно отправить деньги срочно, то можно пользоваться и им (банковский перевод идет один-два дня, через Western Union — гарантированно один день).

Минимальный размер комиссий устанавливается на вывод рубля и гривны. Правда, с гривной система работает только через банк. Если тебе нужно получить деньги на почте, воспользуйся обменником. Основной сайт для Украины — www.webmoney.ua. Там ты найдешь всю информацию по выводу гривны из системы.

Рассмотрим небольшой пример обмена на примере www.webmoney.ua. Предположим, ты хочешь преобразовать доллары в гривну и получить все это банковским переводом. Заходишь на сайт любого обменника (таких много, тарифы у всех разные — на обсуждение всех не хватит и журнала). Обычно тариф составляет от 4 до 10% в зависимости от суммы и способа перевода.

В каждом обменнике должен быть информационный курс обмена одной валюты на другую (как правило, его устанавливают каждый день). В данном случае информационный курс равен 5,10 (при обмене WMZ на гривну).

Предположим, ты хочешь перевести 300 WMZ. Считаем: $300 \times 5,10 = 1530$ грн. Теперь смотрим тарифы обменника. Банковский перевод, сумма от 175-ти до 541-го WMZ, комиссия составляет 4,20%. Умножаем 1530 на 0,042, получаем 64 грн. 26 коп. Итого банковским переводом ты получишь 1530 — 64,26 = 1465 грн. 74 коп.

«Яндекс.Деньги» Принципиальных отличий от Webmoney практически нет. Способом ввода-вы-

В МОСКВЕ КАРТОЧКИ «ЯНДЕКС.ДЕНЬГИ» ОБЫЧНО ПРОДАЮТСЯ С НАЦЕНКОЙ 6%

МИНИМАЛЬНЫЙ РАЗМЕР КОМИССИИ В WEBMONEY УСТАНАВЛИВАЕТСЯ НА ВЫВОД РУБЛЯ И ГРИВНЫ

вода денег в системе достаточно много. Ниже представлены основные способы пополнения счета в электронной платежной системе «Яндекс.Деньги».

пополнить счет можно следующими способами:

- ПРЕДОПЛАЧЕННОЙ КАРТОЧКОЙ;
- НАЛИЧНЫМ ПЕРЕВОДОМ (ОН ЖЕ ПОЧТОВЫЙ);
- ЗАЧИСЛЕНИЕМ ИЗ ДРУГИХ СИСТЕМ (ЧЕРЕЗ ОБМЕННИК);
- БАНКОВСКИМ ПЕРЕВОДОМ.

Первый способ удобен не всегда, ты можешь не найти этих карт в своем городе. В Москве такие карточки продаются с наценкой 6%, например покупаясь карточку на 1000 рублей, а должен заплатить за нее 1060.

С почтовым переводом все ясно — почта везде одна и та же. За перевод обычно берут 3%, но не менее семи рублей. В отличие от WebMoney, «Яндекс.Деньги» позволяет отправить деньги как обычным почтовым, так и электронным почтовым переводом. Если ты воспользуешься обычным почтовым переводом, то он будет идти от двух до пяти рабочих дней. Если же электронным, то средства будут зачислены уже на следующий день. В общем, с почтой разобрались.

Теперь перейдем к банковскому переводу. Размеры комиссий различаются в зависимости от типа банка. Обычно расценки такие же, как и при использовании WebMoney (см. выше). Банковский перевод идет, как правило, один-два дня. Если рядом с тобой есть отделение «Телебанка», ты можешь отправить деньги и вовсе без комиссии.

Вывод денег стоит дороже их ввода. Система взимает комиссию в размере 3% (плюс десять рублей за безналичный банковский перевод) от выводимой суммы, добавляется стоимость агента, через которого будут выводиться деньги (банк, почта). Вывести деньги можно тремя способами:

- БАНКОВСКИМ ПЕРЕВОДОМ;
- ПОЧТОВЫМ ПЕРЕВОДОМ;
- НАЛИЧНЫМИ В ОФИСЕ (АДРЕСА ТЫ УЗНАЕШЬ НА САЙТЕ money.yandex.ru).

Выбирать тебе. Если у тебя открыт счет в банке, воспользуйся банковским переводом иними деньги в банкомате. Почтовым переводом — получишь деньги на почте, но смотри, чтобы не вышло дороже (тут сравнивай комиссию банка и почты). Однако, если суммы небольшие, большой разницы не будет. При осуществлении банковского перевода помни, что некоторые банки также взимают свою комиссию, правда небольшую — обычно 1%.

Третий способ, конечно, подходит не всем. Получить наличные можно только в Москве и Санкт-Петербурге (не будешь же через всю страну ехать). Если ты живешь именно в одной из столиц, то помни, что комиссия при выводе средств все равно составит 3%.

эксперт лицом

ОДНИМ ИЗ ПРИЗНАННЫХ ГУРУ ЭЛЕКТРОННЫХ ДЕНЕГ ПО ПРАВУ СЧИТАЕТСЯ РОБЕРТ ХЕТИНГ. ОН ЯВЛЯЕТСЯ ИЗОБРЕАТЕЛЕМ МНОЖЕСТВА ТЕХНОЛОГИЙ И ОСНОВАТЕЛЕМ НЕСКОЛЬКИХ КОМПАНИЙ, РАБОТАЮЩИХ НА ЭТОМ РЫНКЕ

таблица вывода наличных

способ	доллар	евро	рубли	гривна
Коммерческий банк	0,8% + 0,3% (КОМИССИЯ АГЕНТА)	0,8% + 0,3% (КОМИССИЯ АГЕНТА)	0,8%	0,8%
Western Union	0,8% + 3% + КОМИССИЯ WESTERUNION	0,8% + 3% + КОМИССИЯ WESTERUNION	—	—
Сбербанк	—	—	0,8%	ЧЕРЕЗ ОБМЕННИК ПУНКТ
Почта	—	—	0,8% + КОМИССИЯ ПОЧТЫ	ЧЕРЕЗ ОБМЕННИК ПУНКТ
Ограничение	50 WMZ	50 WME	1500 WMR	250 WMU

С НИМИ удобно?

USABILITY-РЕЙТИНГ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

КАКАЯ ЭЛЕКТРОННАЯ ПЛАТЕЖНАЯ СИСТЕМА САМАЯ УДОБНАЯ? СЕЙЧАС ПОПРОБУЕМ ВЫЯСНИТЬ. НО ЧТОБЫ ТОЧНО СКАЗАТЬ, НАПРИМЕР, ЧТО СИСТЕМА X — САМАЯ-САМАЯ, НУЖНО ОБОСНОВАТЬ ЭТО. ТАК ЧТО С САМОГО НАЧАЛА ПОГОВОРИМ О МЕТОДИКЕ СОСТАВЛЕНИЯ РЕЙТИНГА. БУДЕМ СРАВНИВАТЬ ЧЕТЫРЕ СИСТЕМЫ: WEBMONEY, CYBERPLAT, «ЯНДЕКС.ДЕНЬГИ» И E-PORT | ДЕНИС КОЛИСНИЧЕНКО (DHSILABS@MAIL.RU)

Для составления рейтинга, мы будем оценивать наши электронные платежные системы по следующим параметрам: популярность, универсальность, функциональность, простота ввода-вывода средств, наличие развитой инфраструктуры, стоимость ввода-вывода средств, анонимность, дополнительные функции. Шкала оценок по каждому параметру пятибалльная, как в школе: максимальный балл «5», минимальный — «2». Такой важный параметр, как безопасность, не рассматриваем, так как этому посвящен целый рейтинг со своей методикой в этом номере. Итак, приступим.

ПОПУЛЯРНОСТЬ СИСТЕМЫ Первым параметром, который мы рассмотрим, является популярность системы. Он, наверное, станет решающим в выборе системы. Зачем выбирать систему, если ей никто не пользуется? Чем больше людей прибегают к услугам системы, тем больше возможностей они получают: например, ты перечислил Иванову деньги за дизайн, а от Петрова получил деньги за сайт, который сделал ты (Иванов рисовал для него дизайн) и т.д. Итак, как определить, популярна ли система? Конечно, по количеству пользователей. Тут все просто: чем больше регистраций, тем популярнее система. Если не известно наличие пользователей — оцениваем приблизительно по обороту. Итак, в системе Webmoney сейчас много больше миллиона (около 1,5 млн.) пользователей, а ее оборот по WMR и WMZ составил в 2004 году \$514,68 млн. В «Яндекс.Деньги» (оборот не раскрывается), по дан-



«ЯНДЕКС.ДЕНЬГИ»
23 ОЧКА

usability-рейтинг платежных систем

ПАРАМЕТР/СИСТЕМА	WEBMONEY	CYBERPLAT	E-PORT	«ЯНДЕКС.ДЕНЬГИ»
Популярность системы	5	4	3	3
Универсальность системы	5	3	2	4
Функциональность	5	4	4	3
Ввод-вывод средств	15	14	7	6
Развитая инфраструктура	5	5	3	3
Стоимость ввода-вывода денег	4	5	4	3
Анонимность	1	0	1	1
Дополнительные функции	1	1	3	0
Итого	41	36	27	23

E-PORT
27 ОЧКОВ

CYBERPLAT
36 ОЧКОВ

WEBMONEY
41 ОЧКО

СYBERPLAT, ЕДИНСТВЕННАЯ ИЗ РАССМАТРИВАЕМЫХ СИСТЕМ, ПРЕДЛАГАЕТ ИНТЕРФЕЙС И ДЛЯ КПК, ОДНАКО ЭТА СИСТЕМА НЕ ПОЗВОЛЯЕТ ПОЛЬЗОВАТЕЛЮ ОСТАВАТЬСЯ АНОНИМНЫМ ПРИ РАБОТЕ В НЕЙ

СУДЯ ПО ОТЗЫВАМ, ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННУЮ ПЛАТЕЖНУЮ СИСТЕМУ WEBMONEY ОЧЕНЬ УДОБНО И ИНТУИТИВНО ПОНЯТНО

ным на октябрь 2004 года (более точных официальных данных пока нет, можно предположить 50% годовой рост), количество пользователей составило 200 тысяч.оборот системы CyberPlat в 2004 году составил \$459 млн., в то время как аналогичный показатель E-port — \$144 млн. Таким образом, получаем следующие оценки: WebMoney — 5, CyberPlat — 4, E-port — 3 и «Яндекс.Деньги» — 3.

универсальность системы Второй параметр — универсальность системы. Такую систему можно использовать для любых платежей: и мобильный телефон оплатить, и коммунальные услуги, купить что-то в интернет-магазине, заплатить кому-то за работу. Самой универсальной является WebMoney: тут платишь куда угодно и принимаешь платежи от кого угодно. На втором месте «Яндекс.Деньги», хотя магазинов, поддерживающих работу с ней, меньше, чем для WebMoney и CyberPlat, но CyberPlat позволяет платить только фиксированным получателям, а «Яндекс.Деньги» — даже обычным абонентам системы. CyberPlat проигрывает в том, что не предоставляет возможность переводить деньги со счета в CyberPlat на счет произвольного интернет-магазина. E-port поддерживает платежи и в офлайне (в некоторых интернет-кафе, салонах связи и просто небольших магазинчиках установлено программное обеспечение «E-port дилер»). Однако в последнее время E-port проводит странную политику. Прекращена конвертация валюты E-port в другие системы, и закрыта возможность внутреннего перевода между пользователями системы. Исходя из всего этого, наши системы получают следующие оценки: WebMoney — 5, «Яндекс.Деньги» — 4, CyberPlat — 3 и E-port — 2.

функциональность Третий рассматриваемый параметр — функциональность. Если система удобна в работе, то она постоянно привлекает новых пользователей. WebMoney предоставляет два интерфейса: классический, выполненный в виде обычного приложения, и web-интерфейс. Пользователь может выбирать тот интерфейс, с которым ему проще работать. Судя по отзывам, использовать WebMoney очень удобно. К тому же можно пополнять счет через SMS. Платежи в Cyberplat можно совершать или через сайт, или через дилерскую сеть. Кроме того, Cyberplat предлагает интерфейс и для КПК, чего нет ни в одной из других систем. Система E-port представляет не только web-интерфейс, но и два дополнительных: WAP и SMS (немаловажно для мобильных пользователей). «Яндекс.Деньги» позаботилась о двух интерфейсах: web- и программа «Интернет.Кошелек». Казалось бы, все нормально, но пользователи отмечают неудобность клиентской программы, сложность переводов и платежей в системе. Теперь будем оценивать. За каждый основной интерфейс будем начислять два балла, за дополнительный — один. Расчет прост: WebMoney = 2 (WM Keeper Classic) + 2 (WM Keeper Light) + 1 (SMS)=5, CyberPlat = 2 (сайт) + 2 (КПК)=4, E-port = 2 (сайт) + 1 (WAP) + 1 (SMS)=4, «Яндекс.Деньги» = 2 (сайт) + 2 («Интернет.Кошелек») — 1 (неудобный интерфейс)=3.

простота ввода-вывода средств Четвертый рассматриваемый параметр — простота ввода-вывода средств. Он зависит от общего количества методов, предусмотренных для этих целей. Поскольку WebMoney — единственная мультивалютная система, для нее я буду учитывать только ввод WMR. Оценить простоту ввода-вывода рубля поможет табличка.

наличие развитой инфраструктуры Наличие развитой инфраструктуры — следующий параметр. В этом номере мы уже не раз говорили о инфраструктуре каждой системы: где можно пополнить счет, вывести

usability-рейтинг платежных систем

КОЛИЧЕСТВО МЕТОДОВ	WEBMONEY	«ЯНДЕКС.ДЕНЬГИ»	CYBERPLAT	E-PORT
Ввод денег	10	4	9	5 (**)
Вывод денег	5	2	5 (*)	2

(*) ИЗ ЭТОЙ СИСТЕМЫ НЕЛЬЗЯ ВЫВЕСТИ НАЛИЧНЫЕ СРЕДСТВА, ИХ МОЖНО ПЕРЕВЕСТИ ПО ОДНОМУ ИЗ ПЯТИ НАПРАВЛЕНИЙ: МОБИЛЬНЫЕ ОПЕРАТОРЫ, ИНТЕРНЕТ-ПРОВАЙДЕРЫ, КОММУНАЛЬНЫЕ ПЛАТЕЖИ, ЦИФРОВОЕ ТЕЛЕВИДЕНИЕ, ФИКСИРОВАННАЯ СВЯЗЬ

(**) СПОСОБЫ ВВОДА СРЕДСТВ: ЧЕРЕЗ БАНК (НАЛИЧНЫЕ ИЛИ БЕЗНАЛ — ЭТО ДВА РАЗНЫХ СПОСОБА), В ОФИСЕ КОМПАНИИ, У АГЕНТОВ E-PORT, БАНКОВСКОЙ КАРТОЙ

деньги, где можно обменять деньги, — поэтому не буду повторяться. Лидером в этой категории стала WebMoney, так как она ориентирована в большей степени на электронную работу, соответственно, для этой системы есть множество обменников. CyberPlat, также лидер в этом плане, ориентирована на дилерскую сеть, действительно огромную. E-port и «Яндекс.Деньги» получают по тройке. Первая — из-за того, что запретила обмен своей валюты на валюты других систем. «Яндекс.Деньги» также пока недостаточно популярна, но инфраструктура довольно развитая. Посмотри хотя бы на предыдущую таблицу: даже E-port имеет больше средств ввода-вывода денег, чем «Яндекс.Деньги».

СТОИМОСТЬ ВВОДА-ВЫВОДА СРЕДСТВ Следующий наш параметр по списку — стоимость ввода-вывода средств. Тут все просто. Чем ниже тарифы, тем выше оценка. Самые низкие тарифы имеет CyberPort, за ввод-вывод денег комиссия с пользователей не взимается вообще. На втором месте WebMoney. Комиссия за каждую операцию составляет 0,8% плюс комиссия агента (банка, почты). Комиссия взимается с отправителя.

В «Яндекс.Деньги», наоборот, комиссия взимается с получателя — 1%, а за вывод средств тебе придется заплатить 3%, плюс 10 рублей (если безналом), плюс комиссия агента. E-port взимает 0,75% + \$0,01 с получателя. Таким образом, ставим оценки по этому параметру: CyberPlat — 5, WebMoney — 4, «Яндекс.Деньги» — 3 и E-port — 4.

анонимность Последний в нашем списке, но не последний по важности параметр — анонимность. Возможность анонимной работы предоставляют WebMoney, «Яндекс.Деньги» и E-port. Все они получают по одному баллу. CyberPlat не позволяет остаться анонимным (но здесь анонимность, в принципе, и не нужна) — ноль баллов. Нужно отметить, что пользователи, отказавшиеся от анонимности, получают привилегии в системе. Например, они могут восстановить свой кошелек в случае потери (повреждения) файлов ключей (WebMoney) и/или при потере пароля (WebMoney, «Яндекс.Деньги»). Об этом ты подробнее можешь почитать в статье «Чей safe лучше?» в этом номере журнала.

Кроме указанных параметров, логично рассмотреть также уникальные сервисы, предоставляемые нашими системами. За одну дополнительную функцию будем начислять один бал. Итого: WebMoney — 1 (пополнение кошелька по SMS), CyberPlat — 1 (интерфейс для КПК), E-port — 3 (модемный доступ, WAP-интерфейс, SMS-интерфейс).

Теперь можно подвести итоги. Максимальное количество баллов набрала WebMoney, недалеко от нее CyberPlat. Результаты «Яндекс.Деньги» и E-port приблизительно одинаковы.

СОВОКУПНЫЙ ВЫБОР

НЕСМОТЯ НА ВСЕ РЕЙТИНГИ, ВАЖНО ПОНИМАТЬ, ЧТО ОПТИМАЛЬНУЮ ЭЛЕКТРОННУЮ ПЛАТЕЖНУЮ СИСТЕМУ МОЖНО ПОДОБРАТЬ ЛИШЬ ПО СОВОКУПНОСТИ ПАРАМЕТРОВ. НАПРИМЕР, ТАКОЙ ОЧЕВИДНО УДОБНЫЙ ДЛЯ ПОЛЬЗОВАТЕЛЯ ПАРАМЕТР, КАК ВОЗМОЖНОСТЬ АНОНИМНОЙ РЕГИСТРАЦИИ И, СООТВЕТСТВЕННО, АНОНИМНОЙ РАБОТЫ, В ДАННОМ РЕЙТИНГЕ ЯВЛЯЕТСЯ СУЩЕСТВЕННЫМ ПЛЮСОМ ЭЛЕКТРОННОЙ ПЛАТЕЖНОЙ СИСТЕМЫ. В ТО ЖЕ ВРЕМЯ ПРИ ОЦЕНКЕ БЕЗОПАСНОСТИ И СОСТАВЛЕНИИ РЕЙТИНГА ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ (ЧИТАЙ СТАТЬЮ «ЧЕЙ SAFE ЛУЧШЕ?» В ЭТОМ НОМЕРЕ) ЭТОТ ПАРАМЕТР ЯВЛЯЕТСЯ СКОРЕЕ ОТРИЦАТЕЛЬНЫМ, ТАК КАК ДАЕТ ЭЛЕКТРОННЫМ МОШЕННИКАМ ОПРЕДЕЛЕННУЮ ЛАЗЕЙКУ



РБК
**ХОСТИНГ
ЦЕНТР**

10%
СКИДКА



АРЕНДА ВЫДЕЛЕННЫХ СЕРВЕРОВ

80 у.е.
мес.

1xCeleron 2.8GHz
512Mb RAM
120Gb SATA HDD

90 у.е.
мес.

1xCeleron 2.8GHz
1Gb RAM
160Gb SATA HDD

100 у.е.
мес.

1xPentium4 2.8GHz
1Gb RAM
160Gb SATA HDD

255 у.е.
мес.

2xXeon 2.8GHz
2Gb RAM
36Gb SCSI HDD

Почему стоит выбрать Хостинг-Центр РБК?

Все очень просто:

- Дата Центр APC InfraStruXure™
- Современное серверное оборудование
- Отсутствие установочной платы
- Высокая скорость соединения с Internet
- Круглосуточная техническая поддержка
- Низкая абонентская плата

Более подробную информацию

можно узнать

по телефону клиентской службы

+7 (095) 363-03-09

или на сайте

<http://hosting.rbc.ru>

ВЗГЛЯД ИЗНУТРИ

ИНТЕРВЬЮ С РАЗРАБОТЧИКАМИ ПЛАТЕЖНЫХ СИСТЕМ

РАЗУМЕЕТСЯ, ПРИ ПОДГОТОВКЕ НОМЕРА, ПОСВЯЩЕННОГО ЭЛЕКТРОННЫМ ДЕНЬГАМ, МЫ НЕ СМОГЛИ ОБОЙТИ ВНИМАНИЕМ ИГРОКОВ ЭТОГО РЫНКА — ТВОЕМУ ВНИМАНИЮ КРУГЛЫЙ СТОЛ С ОСНОВНЫМИ ИЗ НИХ. НА ВОПРОСЫ СПЕЦА ОТВЕЧАЕТ ГЛАВНЫЙ РЕДАКТОР «ЯНДЕКСА» ЕЛЕНА КОЛМАНОВСКАЯ, ИСПОЛНИТЕЛЬНЫЙ ДИРЕКТОР ГРУППЫ E-PORT АЛЕКСАНДР ПОКРОВСКИЙ И ДИРЕКТОР ПО ВНЕШНИМ СВЯЗЯМ КОМПАНИИ WEBMONEY TRANSFER ПЕТР ДАРАХВЕЛИДЗЕ. ДЛЯ УДОБСТВА МЫ РАЗБИЛИ ВСЕ ВОПРОСЫ НА НЕСКОЛЬКО ГРУПП | АШОТ ОГАНЕСЯН (ASHOT@REAL.HAKER.RU)

1 состояние рынка и перспективы его развития

**XS: КАК ВЫ ОХАРАКТЕРИЗУЕТЕ ТЕКУЩЕЕ СОСТОЯНИЕ
ОТЕЧЕСТВЕННОГО РЫНКА ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ?**

ЕЛЕНА КОЛМАНОВСКАЯ: Состояние рынка платежных систем сегодня можно охарактеризовать как «в начале бурного развития». Электронные платежи — это закономерный этап в развитии телекоммуникаций. Электронные платежи нужны в первую очередь для покупки услуг и нематериальных товаров, «отгружаемых» через интернет. Как электронная почта избавляет от необходимости ходить на почту для отправки писем, так и электронные платежи экономят время и усилия. Очевидно, что скорость распространения электронных платежей зависит

Елена Колмановская
главный редактор
компании «Яндекс»



не только от развития самих платежных систем, но и от расширения доступа населения к интернету. Сейчас в России интернет-пользователей более 20-ти миллионов, из них половина пользуется Сетью не реже раза в неделю и чуть больше четверти — ежедневно. Рост аудитории интернета — четыре-пять миллионов пользователей в год. Кроме того, с развитием broadband-соединений увеличивается частота использования интернета, пользователи чаще обращаются к интернету, и, что еще более важно, обращение к Сети психологически становится даже проще, чем звонок по телефону. Естественно, все это стимулирует рост платежных систем.

АЛЕКСАНДР ПОКРОВСКИЙ: Я считаю, что здесь все достаточно тривиально. Текущее состояние развития рынка отвечает его текущим потребностям. Появятся новые потребности — будут усовершенствованы сервисы.

ПЕТР ДАРАХВЕЛИДЗЕ: Рынок все еще молодой, бурно развивающийся и недостаточно насыщенный. Своей платежной системой пытается обзавестись практически каждый портал или интернет-холдинг. Это говорит о том, что люди видят здесь перспективу и они уверены в том, что у них есть нечто новое, что они хотят предложить пользователю. В интернете появляется все больше таких принципиально новых покупок и таких услуг, «традиционного взгляда» на которые никогда не существовало. Кому-нибудь, например, придет в голову оплачивать меч и доспехи из «Арены» или персонаж в Warcraft через «Сбербанк»? Нет, никогда. Для очень многих молодых людей электронные платежи — первый, лучший и единственный способ произвести оплату в Сети.

Мы думаем, что через восемь-десять лет уже можно будет оперировать термином «неотъемлемые».

XS: НАСКОЛЬКО КОРРЕЛИРУЕТ РАЗВИТИЕ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ В РОССИИ С РАЗВИТИЕМ ИХ ИНОСТРАННЫХ АНАЛОГОВ? КАКОВА ДИНАМИКА ПОТРЕБЛЕНИЯ УСЛУГ ИНТЕРНЕТ-ПЛАТЕЖЕЙ В ДАЛЬНЕМ ЗАРУБЕЖЬЕ?

ЕЛЕНА КОЛМАНОВСКАЯ: На Западе больше распространены кредитки и интернет-банкинг. Основной принцип работы с кредитками — подтверждение платежа личной уникальной подписью. В интернете биомеханической подписи никто не оставляет, поэтому некоторое недоверие к кредиткам при платежах в Сети испытывают и покупатели, и продавцы. Для снятия напряжения, например, существует система PayPal.

АЛЕКСАНДР ПОКРОВСКИЙ: Как я уже говорил, состояние рынка отвечает его потребностям. На Западе одни потребности и один уровень развития, у нас другие — и другой уровень. Единственное, что можно добавить: в мире действительно значительно больше распространены операции с кредитными карточками.

ПЕТР ДАРАХВЕЛИДЗЕ: Вполне коррелирует. В мире активно развиваются как банковские, так и небанковские платежные системы, что наблюдается и у нас. В каких-то нишах нашему развитию в России мешает отсутствие законодательной базы. Это, например, ситуация с электронными билетами (в Европе и США они уже почти вытеснили бумажные, а у нас еще не появились) или проблемы с авторскими правами, которые мешают развитию рынка электронных книг и других медиа.

XS: КАКОВЫ, НА ВАШ ВЗГЛЯД, КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА ОНЛАЙНОВЫХ ПЛАТЕЖЕЙ В СРАВНЕНИИ С ТРАДИЦИОННЫМИ СПОСОБАМИ?

ЕЛЕНА КОЛМАНОВСКАЯ: У кредиток есть и еще одна проблема: они не годятся для микроплатежей, так как слишком велика стоимость транзакции с их помощью. То есть покупать, например, отдельные музыкальные композиции (треки) стоимостью в пределах доллара по кредитке невыгодно. Таким образом, преимущество электронных денег перед кредитками — это безопасность и возможность работы со сколь угодно маленькими суммами. Кроме того, электронные платежные системы представляют определенный общественный интерес как альтернатива наличного оборота: они лучше контролируются и регулируются.

АЛЕКСАНДР ПОКРОВСКИЙ: Безусловно, это скорость. Если, например, ты хочешь прочитать какую-то статью в электронном виде, получить доступ к какой-то информации, но для этого требуется оплата, то электронная платежная система, в отличие от традиционных способов оплаты, позволяет сделать это практически мгновенно. Кроме того, для других участников системы налицо экономия времени и сил на обработку платежа тех организаций, в адрес которых эти платежи поступают. Собственно, я думаю, что вообще нет смысла разделять платежи на электронные и неэлектронные. Как известно, сейчас все платежи электронные. Ты приходишь в Сбербанк, и при этом для нет никакой разницы с обращением к электронной платежной системе: в Сбербанке стоит компьютер, идет информация в ЦБ, еще куда-то. В любом случае это электронная платежная система на сегодня. Другой разговор начинается, когда нужно отличить наличные и безналичные платежи. Во втором случае все очевидно: во-первых, не нужно

держат в кармане наличные; во-вторых, можно быстро распорядиться своими деньгами, никуда не выходя из дома. Элементарная экономия времени, которое, как известно, — деньги.

ПЕТР ДАРАХВЕЛИДЗЕ: Для цифровых товаров онлайн-платежи являются, безусловно, лучшим способом оплаты, здесь даже преимущества сравнивать смешно. Для оплаты покупок во многих российских интернет-магазинах люди идут на почту или в банк, потом ждут неделю, чтобы после прихода денег за минуту скачать оплаченную информацию или программу, — это анахронизм. Нам он показывает, насколько еще неразвит российский рынок платежных систем и как много здесь работы. Для товаров с физической доставкой ситуация совершенно другая. Для простых товаров (книги, диски и т.п.) онлайн-оплата — это удобная опция, если покупатель не может расплатиться с курьером, например в силу географической удаленности. Онлайн-оплата дорогих и индивидуальных товаров (бытовая техника, одежда) — это, скорее, дань моде. Если для продавца таких товаров предоплата (даже электронными деньгами) всегда является плюсом, то для покупателя в этом случае преимущества еще надо как следует поискать.

XS: КАКОВА ВОСТРЕБОВАННОСТЬ УСЛУГ ИНТЕРНЕТ-ПЛАТЕЖЕЙ НА РОССИЙСКОМ РЫНКЕ? СКОЛЬКО ВРЕМЕНИ, ПО ВАШИМ ОЦЕНКАМ, ПРОЙДЕТ, ПРЕЖДЕ ЧЕМ НОВАЯ УСЛУГА «ПРИЖИВЕТСЯ» У ПОТЕНЦИАЛЬНЫХ КЛИЕНТОВ?

ЕЛЕНА КОЛМАНОВСКАЯ: Можно утверждать, что системы электронных платежей уже вполне прижились. Ими пользуются сотни тысяч людей в России. Тем не менее, эти пользователи все еще в большинстве своем early adopters, так как мы знаем, что интернетом пользуются миллионы. Именно поэтому мы видим большой потенциал развития.

АЛЕКСАНДР ПОКРОВСКИЙ: Сами по себе системы платежей не предоставляют новых услуг как таковых, а возникают по мере того, как появляются услуги, для которых важна оперативность. Таких отраслей пока немного, но очевидно, что со временем их будет больше. Сам пользователь может оценить себя и понять, насколько нужно ему «то или иное». Я, например, активно пользуюсь интернет-магазинами, и объем моих покупок в них нередко превышает объем покупок в обычных магазинах, потому что это просто экономит мое время. Но, как правило, мне там совершенно не нужно расплачиваться «электронно». А то, что мне нужно, я покупаю «электронно». Не больше, не меньше. Я думаю, с определенной долей вероятности это легко экстраполировать на весь рынок.

ПЕТР ДАРАХВЕЛИДЗЕ: Востребованность высока в тех нишах, где есть полноценный продукт — цифровой товар, чьи свойства хорошо «накладываются» на свойства онлайн-платежа: моментальность оплаты, моментальность доставки, простота и безотзывность. Например, многие хостинговые компании уже полностью строят свой бизнес в нашей системе: они получают WebMoney за свои услуги и тратят их на web-рекламу, оплачивают трафик, платят зарплату программистам и дизайнерам, делают покупки у продавцов hardware и т.п. То есть востребованность, как видим, может быть стопроцентной, причем без всяких усилий на продвижение и раскрутку.

XS: КАКОВА СТРУКТУРА ДОХОДОВ ВАШЕЙ ПЛАТЕЖНОЙ СИСТЕМЫ? НА КАКИЕ ПЛАТЕЖИ ПРИХОДИТСЯ ОСНОВНОЙ ДОХОД?

ЕЛЕНА КОЛМАНОВСКАЯ: Основной источник дохода — комиссии с продажи товаров и услуг. Наиболее востребованные платежи — за нематериальные товары (услуги), то есть телефонная связь (мобильная, международная и междугородняя), интернет-услуги (реклама, доступ в интернет и хостинг), коммерческое телевидение и т.д.

АЛЕКСАНДР ПОКРОВСКИЙ: Подавляющее большинство платежей приходится на оплату услуг сотовой связи.

ПЕТР ДАРАХВЕЛИДЗЕ: У нас простая и очевидная структура доходов: комиссия с каждой транзакции в размере 0,8%, но не более 50 WMZ и 1500 WMR. Это удобно и нам, и нашим клиентам: кто ведет бизнес в WebMoney, тот понимает, что он платит единственный и не слишком обременительный «налог» со своей деятельности. Именно поэтому большая часть наших доходов приходится на р2р-платежи.

2 защита информации

XS: ОДИН ИЗ НАИБОЛЕЕ АКТУАЛЬНЫХ ВОПРОСОВ, КОТОРЫЕ ВОЛНЮТ ПОЛЬЗОВАТЕЛЕЙ, — ЭТО ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ. КАК ОБСТОЯТ ДЕЛА С ЭТИМ ПАРАМЕТРОМ? КАКИМ ОБРАЗОМ ВАША СИСТЕМА ГАРАНТИРУЕТ БЕЗОПАСНОСТЬ ТРАНЗАКЦИЙ? ИЗВЕСТНЫ ЛИ СЛУЧАИ ВЗЛОМА ИЛИ ХИЩЕНИЯ ЧУЖИХ СРЕДСТВ?

ЕЛЕНА КОЛМАНОВСКАЯ: Проблемы с безопасностью можно разделить на две части: с одной стороны, собственная внутренняя безопасность системы, то есть устойчивость к взлому, с другой стороны — мошенничество, которое совершается с использованием системы. По первой позиции современные системы электронных платежей намного обогнали кредитные карты, так как при создании электронных платежных систем был учтен большой исторический опыт. Технология PayPal, на базе которой построена система «Яндекс.Деньги», лицензирована целому ряду компаний для различных применений. Ядро системы прошло неоднократные экспертизы в России и за рубежом, на технологию выдан ряд патентов. Случаи ее взлома нам неизвестны. «Внешние» проблемы, как правило, связаны с недобросовестностью продавца. Типичная жалоба: «Я перевел деньги, а товара не получил». В этом случае администрация системы «Яндекс.Деньги» готова помочь потерпевшему всеми имеющимися у нее данными. Хотя в этой ситуации система электронных платежей виновата не больше, чем ЦБ виноват в том, что покупатель приобрел некачественный товар за наличные деньги или проиграл их в лототроне. Предупреждать мошенничества позволяет аналитическая работа службы безопасности. Кроме того, на сайте системы «Яндекс.Деньги» есть торговый ряд, где перечислены только те партнеры системы (поставщики товаров и услуг), с которыми заключены договоры. Таким образом мы «говорим» пользователю, что это магазины, которые работают официально — они были вчера и не исчезнут завтра.

АЛЕКСАНДР ПОКРОВСКИЙ: Мы гарантируем адекватность системы безопасности хранимым деньгам. То есть сам канал, по которому мы обмениваемся с клиентом информацией, защищен 128-битным ключом для тех, кто за этим следит. Для тех, кто не следит, — 56. Я уверю, что для взлома SSL-соединения даже в 56 бит нужно потратить не одну сотню долларов, а на 128 бит — значительно больше. И ты взламываешь при этом одну сессию. Причем ты никогда не сможешь реально воспользоваться этим знанием, для того чтобы успешно взломать другое SSL-соединение. Вообще же самым уязвимым местом является компьютер пользователя. То есть, если к пользователю внедрили троян какой-то, который «пишет» клавиатуру и потом отправляет ее куда-то, то этой жертве не поможет ничего. Естественно, в это место бьют чаще всего. Но в данном смысле наша система по защите полностью эквивалентна любой системе на клавиатурных комбинациях.

ПЕТР ДАРАХВЕЛИДЗЕ: Если бы дела обстояли плохо, мы бы с Вами не беседовали. WebMoney одной из первых на российском рынке, еще в 1998 г., взяла на вооружение асимметричные криптографические алгоритмы, цифровую подпись и другие средства защиты данных. Все переводы средств действительно представляют собой транзакции на уровне базы данных: средства попадают на кошелек получателя, только если они списаны с отправителя, одной операцией. Поэтому у нас никогда не было путаницы со счетами, пропадания или «удвоения» денег, которыми грешили даже очень крупные и известные международные системы.

XS: КАКИЕ МЕТОДЫ РАЗГРАНИЧЕНИЯ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ ИСПОЛЬЗУЮТСЯ, ПОМИМО ТРАДИЦИОННОГО ПАРОЛЯ?

ЕЛЕНА КОЛМАНОВСКАЯ: Большинство пользователей соглашаются на стандартный уровень безопасности ради удобства работы с web-кошельком — то есть работать просто через браузер. При этом у них, кроме обычного пользовательского пароля, есть еще и защищенный платежный пароль. Те, кто ради дополнительного уровня защиты готовы пойти на дополнительные ограничения, могут установить у себя на компьютере специальную программу-кошелек, которая дополнительно шифрует данные о транзакциях.

АЛЕКСАНДР ПОКРОВСКИЙ: Для корпоративных клиентов используется 1024-битный сертификат, для мобильных телефонов — 512-битные ключи. Сейчас мы обдумываем вопрос использования ЭЦП для частных клиентов. Но здесь есть ряд сложностей. А вообще (я в очередной раз повторюсь) уровень защиты адекватен хранимым суммам. В подавляющем большинстве случаев для обеспечения защиты вполне хватает SSL-соединения с достаточно длинным ключом.

ПЕТР ДАРАХВЕЛИДЗЕ: Классический пароль, с нашей точки зрения, полностью дискредитировал себя как средство разграничения доступа. Вообще, вся информация, хранящаяся на компьютере пользователя, потенциально уязвима. Нужно исходить из того, что существующие и еще не найденные «дырки» в программах и протоколах, рано или поздно они позволят взломщику получить доступ к персональным данным среднестатистического пользователя. Но если защитить информацию на компьютере невозможно, значит... ее там не должно быть. Именно так работает наш метод аутентификации e-num (enum.ru). Пользователю выдается уникальный одноразовый шифроблокнот в виде сгенерированного специально для него Java-мидлета для мобильного телефона или программы для КПК. При входе в защищенную зону тебе посылают число-запрос, а ты получаешь с мобильника число-ответ. Таким образом можно пользоваться WM Кеерг и другими сервисами, которые используют e-num, из любого, даже самого ненадежного интернет-кафе или клуба. Твою персональную информацию выудят только вместе с мобильником, а это уже совершенно другая статья Уголовного кодекса, в отличие от рассылки троянов и установки кейлоггеров.

XS: КАКИЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ ПРИМЕНЯЮТСЯ ДЛЯ ЗАЩИТЫ ПЛАТЕЖЕЙ? КАК ВООБЩЕ ОБЕСПЕЧИВАЕТСЯ ШИФРОВАНИЕ ТРАНЗАКЦИЙ?

Петр Дарахвелидзе,
директор по внешним
связям компании
WebMoney Transfer



ЕЛЕНА КОЛМАНОВСКАЯ: Методы, используемые в технологии PayCash, защищены четырьмя патентами РФ. Они были представлены на международных конференциях и получили высокие оценки от таких специалистов по криптографии, как Брюс Шнайер и Дэвид Чаум. Для обеспечения безопасности участников системы «Яндекс.Деньги» используются такие методы защиты информации, как метод представления денежных обязательств, защищенный патентом «Способ проведения платежей (варианты)», хэш-функции, генераторы случайных чисел, контроль целостности критических данных при помощи CRC и пр.

АЛЕКСАНДР ПОКРОВСКИЙ: Несмотря на то, что при использовании SSL особой нужды в шифровании транзакций не возникает, мы все же иногда делаем это, но по большому счету вся остальная информация нормально защищена тем же SSL. Мы используем шифрование только в некоторых наших приложениях типа мобильной коммерции для обычного мобильного телефона. SSL поддерживается только на достаточно дорогих моделях. А мы хотим, чтобы «с нами» можно было работать с более дешевой моделью, поэтому используем методы шифрования, отличные от SSL. Я не хочу вдаваться в подробности о том, какие именно, но они адекватны и, в общем, эквивалентны тому же SSL. А вообще суть вопроса в том, что важно не КАКИЕ методы кто-то использует, а КАК он это делает. Здесь можно говорить долго. Но в целом корректно примененного SSL encode вполне достаточно. Для больших денег можно использовать сертификат.

ПЕТР ДАРАХВЕЛИДЗЕ: Мы не раскрываем применяемых нами алгоритмов. Следует только сказать, что среди них нет проприетарных, изобретенных «на коленке» алгоритмов.

3 перспективы развития

XS: КАК ВЫ ОЦЕНИВАЕТЕ ДАЛЬНЕЙШИЕ ПЕРСПЕКТИВЫ РАЗВИТИЯ РЫНКА ПЛАТЕЖНЫХ ИНТЕРНЕТ-СИСТЕМ? НА КАКИЕ УСЛУГИ, ПО ВАШИМ ПРОГНОЗАМ, БУДЕТ РАСТИ СПРОС?

ЕЛЕНА КОЛМАНОВСКАЯ: Рыночная ниша платежных систем очень понятна. Людям нужен инструмент для быстрых платежей в интернете за товары и услуги. Интернет-банкинг напрямую тут не спасает: каждому банку пришлось бы подключаться к тысячам поставщиков товаров и услуг. Карты не работают, потому что высок уровень мошенничества, и, кроме того, их процессинг стоит значительно дороже, чем процессинг интернет-платежей. Таким обра-

Александр
Покровский, испол-
нительный директор
группы e-port



зом, нужна модель, сочетающая единый процессинговый центр (как у карт — и при этом независимый, чтобы нормально взаимодействовать с банками) и безопасность (на уровне интернет-банкинга). Все это должно быть доступно отовсюду и 24 часа в сутки (а не только в «банковские» часы). Собственно, так и получается модель «Яндекс.Деньги». А раз эта модель нужна, значит, будет развиваться. В первую очередь растет спрос на услуги нематериальные. Например, уже в этом году многие банки поняли преимущества интернет-платежей и готовы начинать более тесно сотрудничать по рознице, в частности, использовать электронные платежи для возврата кредитов.

АЛЕКСАНДР ПОКРОВСКИЙ: На мой взгляд, основное развитие придется на те сферы, где потребителю нужна какая-то информация, где он покупает какой-то контент.

ПЕТР ДАРАХВЕЛИДЗЕ: В ближайшие годы вполне реальны ежегодные приросты в несколько раз. Базой для такого прогноза являются высокие темпы роста числа пользователей интернета и рунета в частности. Для этой аудитории в онлайн будут переноситься все новые услуги из офлайна, а вдобавок многие ранее бесплатные в интернете товары и услуги будут становиться платными. Например, услуги Wi-Fi пока часто предоставляются бесплатно в рекламных и тестовых целях, а в ближайшем будущем онлайн-биллинг Wi-Fi станет важнейшей платной услугой.

XS: РАССКАЖИТЕ О ТЕХ ПРОДУКТАХ, КОТОРЫЕ В ВАШИХ КОМПАНИЯХ ВЫПУСКАЮТСЯ ДЛЯ ОСВОЕНИЯ НОВЫХ СЕКТОРОВ РЫНКА.

ЕЛЕНА КОЛМАНОВСКАЯ: Мы считаем, что «Яндекс.Деньги» — это продукт для всех. В пресс-релизе «Каждому пользователю «Яндекса» — электронный кошелек» мы формулировали это так: «Не только для профессионалов интернета, но и для их начальников, секретарей, детей и родителей». Наша задача — сделать платежи привычными и стандартными, то есть сделать их частью регулярного интернет-пейзажа.

АЛЕКСАНДР ПОКРОВСКИЙ: Мы готовим выпуск продукта, который облегчит подключение интернет-магазинов к нашей системе. Дальше упоминания продукта я пока детализировать не могу.

ПЕТР ДАРАХВЕЛИДЗЕ: Мы развиваем направление электронных книг — проект publicant.ru. Оказывается, отношение к авторам и их правам не такое нигилистическое, как может показаться на первый взгляд. Новая книга автора «Ночного дозора» С.Лукияненко появилась у нас раньше бумажной версии и разошлась почти тысячей экземпляров ценой в 1 WMZ каждая. Да, появилась эта книга и у пиратов, да, многие по привычке скачали ее «на халяву». Но задумаемся на минуту: разве ты пожелаешь отдать небольшую сумму любимому писателю, особенно зная, что он получит 95% от нее? В ближайшие годы предстоит борьба за сердца и умы читателей электронных книг. И выиграть ее мы собираемся не за счет запретов и репрессий, а за счет предложения качественного продукта по разумной цене. А разговоры о том, что за хорошую книгу нельзя или не хочется отдать 1 WMZ, пусть ведут неудачники. У нас еще много новых проектов и сервисов: система массовых платежей MassPayment, коллективная WM-бухгалтерия Capitaler, кредитная биржа и кредитный рейтинг. Критерий успешности у всех один: проекты должны заинтересовывать новых пользователей в услугах системы и повышать лояльность существующих клиентов. А если есть пользователи, будет и финансовый результат.

У НАС ОЧЕНЬ БОЛЬШОЙ

ВЫБОР

* В нашем магазине вас ждет более 1000 игр на ваш выбор

* Постоянно обновляемый ассортимент



Guild Wars

\$69.99



Grand Theft Auto: San Andreas (PC-DVD)

\$69.99



F.E.A.R. (Director's Cut Edition)

\$19.99



Black & White 2

\$19.99



City of Heroes Collectors DVD Edition

\$89.99



Quake 4

\$75.99



World of Warcraft (UK Version)

\$59.99



Star Wars Galaxies: The Total Experience (EURO)

\$59.99



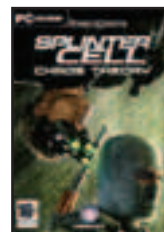
Sid Meier's Civilization III Complete

\$59.99



Baldur's Gate Original Saga

\$49.99



Splinter Cell: Chaos Theory

\$79.99



Fable: The Lost Chapters

\$79.99

Играй просто!
GamePost

ЗАБУДЬ ПРО ТЕЛЕЖКИ

МЫ ПРИВЕЗЕМ ВСЕ САМИ!



Тел.: (095) 780-8825
Факс.: (095) 780-8824

www.gamepost.ru



старые добрые пластиковые карты

ЧЕМ ПОЛЬЗУЮТСЯ МОШЕННИКИ

СРЕДСТВА И МЕТОДЫ ЗАЩИТЫ ПЛАСТИКОВЫХ КАРТ ОЧЕНЬ РАЗНООБРАЗНЫ, ИМ ПОСВЯЩЕНО МНОЖЕСТВО ПУБЛИКАЦИЙ, НО МЫ ОСТАНОВИМСЯ ТОЛЬКО НА ТЕХНИЧЕСКОЙ СТОРОНЕ ВОПРОСА **АНДРЕЙ МЕЖУТКОВ**



классификация карт С виду все карточки похожи и кажутся совершенно одинаковыми, разве что разный окрас и информация на них. Различий гораздо больше.

по виду носителя (собственно карты):

- СО ШТРИХ-КОДОМ (В ТОМ ЧИСЛЕ КАРТЫ ПРЕДОПЛАТЫ, НА НИХ КЛЮЧ ДЛЯ ПОПОЛНЕНИЯ СЧЕТА СКРЫТ СПЕЦИАЛЬНЫМ СТИРАЮЩИМСЯ ЗАЩИТНЫМ СЛОЕМ).
- С МАГНИТНОЙ ПОЛОСОЙ (ВЫСОКОКОЭЦЕРТИВНОЙ ИЛИ НИЗКОКОЭЦЕРТИВНОЙ, С ЗАПИСЬЮ НА ЛЮБУЮ ИЗ ТРЕХ ДОРОЖЕК).
- ЧИП-КАРТЫ (КАРТЫ С ПЗУ; КАК ПРАВИЛО, ЭТО ПРЕДОПЛАЧЕННЫЕ ТЕЛЕФОННЫЕ КАРТЫ БЕЗ ВОЗМОЖНОСТИ ПОПОЛНЯТЬ ИХ).
- СМАРТ-КАРТЫ (КАРТЫ И БРЕЛОКИ С МИКРОПРОЦЕССОРОМ И ЗАЩИЩЕННОЙ ПАМЯТЬЮ, К НИМ ОТНОСЯТСЯ РАСПРОСТРАНЕННЫЕ СЕЙЧАС FLASH-КАРТЫ, SIM-КАРТЫ, МНОГОЧИСЛЕННЫЕ ВАРИАЦИИ НА ТЕМУ TOUCH-MEMORY И IBUTTON).
- БЕСКОНТАКТНЫЕ КАРТЫ (В ТОМ ЧИСЛЕ РАЗНЫЕ БРЕЛОКИ PROXIMITY CARDS, РАБОТАЮЩИЕ В НАВЕДЕННОМ ЭЛЕКТРОМАГНИТНОМ ПОЛЕ).

Пластиковые карты можно классифицировать и по уровню реакции карты или по степени «умности». Тогда мы получаем идентификационные карты, с которых определенным методом (магнитной головкой, в электромагнитном поле, оптическим штрих-кодовым считывателем) считывается идентификатор, привязанный к сервису для владельца этой карты. Например, с помощью такой карты ее пользователь получает разрешение войти в помещение или списать сумму за проезд в общественном транспорте или по платной дороге. Действие данного вида карт распространяется и на «электронные кошельки», при их использовании вся информация об услуге, к примеру о доступной для пользователя сумме, находится прямо на карте. Непосредственно на идентификационных картах находится и соответ-

ствующее программное обеспечение, значит, карточку можно «нагрузить» дополнительными защитными функциями, что, как правило, не ухудшает потребительские свойства карты, но в то же время сильно усложняет жизнь атакующему. Кроме того, такое техническое решение удешевляет инфраструктуру по обслуживанию карт: не требуются постоянные выделенные каналы от точки обслуживания к процессинговому центру или, в более общем случае, к банку-эмитенту (который выпустил карту в оборот) и банку-эквайеру (который ответствен за точку обслуживания).

можно классифицировать карты и по области их применения:

- КАРТЫ ДОСТУПА (ДЛЯ УЧЕТА РАБОЧЕГО ВРЕМЕНИ СОТРУДНИКА ИЛИ ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К ГОСТИНИЧНОМУ НОМЕРУ ГОСТЕМ).
- БАНКОВСКИЕ КАРТЫ (В ЗАВИСИМОСТИ ОТ ВИДА СЧЕТА ОНИ МОГУТ БЫТЬ КРЕДИТНЫМИ И ДЕПОЗИТНЫМИ).
- ДИСКОНТНЫЕ КАРТЫ.
- КЛУБНЫЕ КАРТЫ.
- ПРЕДОПЛАЧЕННЫЕ ТЕЛЕФОННЫЕ КАРТЫ.
- КАРТЫ ДЛЯ ПРОЕЗДА НА МЕТРО ИЛИ ИНОМ ТРАНСПОРТЕ.
- КАРТЫ ДЛЯ ОПЛАТЫ УСЛУГ ПРОВАЙДЕРОВ МОБИЛЬНОЙ СВЯЗИ И ИНТЕРНЕТА.
- КАРТЫ — ДЕШИФРАТОРЫ СИГНАЛОВ ПЛАТНОГО ТЕЛЕВИДЕНИЯ.
- ИДЕНТИФИКАЦИОННЫЕ КАРТЫ ЛИЦЕНЗИРОВАННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.

Каждый описанный класс можно детализировать, придумать еще несколько видов классификации, но мы пойдем дальше.

Мы уже договорились о том, что статья посвящена технической стороне работы пластиковых карт, поэтому ее предметом станут карты, которые можно считать самыми опасными в плане последствий их использования. Конечно, в первую очередь к таким относятся банковские и SIM-карты, то есть те, которые выше я классифицировал как «смарт» (англ. smart — «умный»).

Начнем с банковских карт с магнитной полосой. Во-первых, они на сегодня составляют подавляющее большинство в общей массе эмиссии, а во-вторых, они гораздо более беззащитны перед атаками.

Противодействие мошенничеству в МПС носит комплексный характер, так как прежде всего сама платежная система имеет довольно сложную географическую и техническую топологию и практически невозможно иметь единый центр по управлению ей. В некотором смысле архитектура МПС напоминает архитектуру интернета: есть домены, роль которых выполняют точки обслуживания (point of sale — точка оплаты или point of service — точка обслуживания) банков-эквайеров. Как некий аналог DNS (Domain Name Server) или маршрутизатора можно рассматривать процессинговый центр, который ориентируется на номер карты (чем не IP-адрес?) и посылает запрос в соответствующий ПЦ данной МПС. При этом, в случае если ПЦ не знает, куда посылать такой запрос, он отправляет его более старшему по иерархии ПЦ — полное соответствие логике маршрутизации в интернете.

Основной способ мошенничества с картами также аналогичен мошенничеству в Сети — использование чужих идентификационных данных. Правда, если в Сети все действия происходят в виртуальном пространстве, то с картами ситуация сложнее и иногда кардерам приходится встречаться с обслуживающим персоналом POS «живьем». Следовательно, добавляется еще один способ кардерства — подделка карты.

Противодействие подделке физического носителя пластиковых карт довольно близко к защите дензнаков. Микрочечка, довольно сложная голограмма, специальный шрифт (обрати внимание на надпись «VISA», особенно на первую букву), полоса для подписи владельца (подпись должна быть одинаковой с подписью в удостоверении личности). Кроме того, в зависимости от типа карты (универсальная или только для электронных расчетов), на ней может быть выдавлена (эмбоссирована) идентифицирующая информация: номер карты, имя владельца, срок действия. Фактически это повторяет информацию, хранящуюся на магнитном слое карты. И хотя каждый банк, эмитирующий карты (выпускающий их в оборот и держащий соответствующие карточные счета), обычно печатает карты с собственным дизайном, перечисленные методы защиты от подделки обязательны на банковских картах по требованиям международных (VISA, EuroPay, MasterCard, American Express, JBL) и российских национальных платежных систем (UnionCard, «Сберкарт», «Золотая Корона»). Эти требования несколько отличаются в различных платежных системах, но в целом соответствуют списку.

Полный перечень методов защиты известен в каждом банке-эмитенте. Часть параметров, которые можно контролировать без применения специальных технических средств, обязательно сообщаются в точки обслуживания. Большинство атак на платежную систему засекают именно продавцы в точках обслуживания, так как они знают признаки подделки карт так же, как и симптомы фальшивых купюр.

Точка обслуживания, снабженная сотрудником, опасна не только как место нападения на платежную систему, но и как место, где мошенничают и сами продавцы в ущерб пользователям-картхолдерам (card holder — владелец карты). С какими целями могут совершаться атаки на держателей карт?

К примеру, чтобы поживиться на «двойном снятии» в пользу точки обслуживания (при ручном обслуживании «двойная прокатка» на слип-машине). Или чтобы продать полученную идентификационную информацию с карты, такая нажива будет легкой по нескольким причинам. Во-первых, эти данные остаются в POS, похищать реквизиты отсюда легко и удобно. Во-вторых, оплата с кредитных карт, привязанных в банке к кредитному виду счета (в отличие от оплаты с депозитных карт), часто не требует проверки состояния счета: на этих картах любая оплата осуществляется в кредит и наличие средств на карте не имеет значения. Плюс сбор идентификационной информации по картам происходит с временными задержками и проверяется относительно трудно, особенно если он производится в ручном режиме. Вот и получаем, что масса мелких «двойных» оплат с различных карт может серьез-

уязвимость популярного стандарта

DES — ЭТО АМЕРИКАНСКИЙ СТАНДАРТ ШИФРОВАНИЯ ДАННЫХ ДЛЯ КОММЕРЧЕСКИХ ПРИЛОЖЕНИЙ. ДЛИНА КЛЮЧА СОСТАВЛЯЕТ 56 БИТ. СТАНДАРТ ВВЕДЕН В ДЕЙСТВИЕ В 1977 ГОДУ. ОТНОСИТЕЛЬНО НЕДАВНО ЗАМЕНЕН НОВЫМ СТАНДАРТОМ AES (ADVANCED ENCRYPTION STANDARD; ИМЕЕТ ДЛИНУ КЛЮЧА В 128 БИТ, ОСНОВАН НА ПЕРСПЕКТИВНОЙ АРХИТЕКТУРЕ «КВАДРАТ»). DES К НАШЕМУ ВРЕМЕНИ МОРАЛЬНО УСТАРЕЛ, ИМЕЕТ МАЛУЮ ДЛИНУ КЛЮЧА И ОРИЕНТИРОВАН, ПРЕЖДЕ ВСЕГО, НА ЭЛЕКТРОННУЮ (СХЕМОТЕХНИЧЕСКУЮ) РЕАЛИЗАЦИЮ, ТАКЖЕ ИМЕЕТ МАССУ 1/4/6-БИТОВЫХ ОПЕРАЦИЙ, ЧТО УСЛОЖНЯЕТ ЕГО ПРОГРАММНУЮ РЕАЛИЗАЦИЮ. ОДНАКО ЭТОТ СТАНДАРТ НАСТОЛЬКО РАСПРОСТРАНЕН В КОММЕРЧЕСКОЙ СФЕРЕ, ЧТО МАССОВЫЙ И БЫСТРЫЙ ПЕРЕХОД НА НОВЫЙ АЛГОРИТМ ОЧЕНЬ СЛОЖЕН.

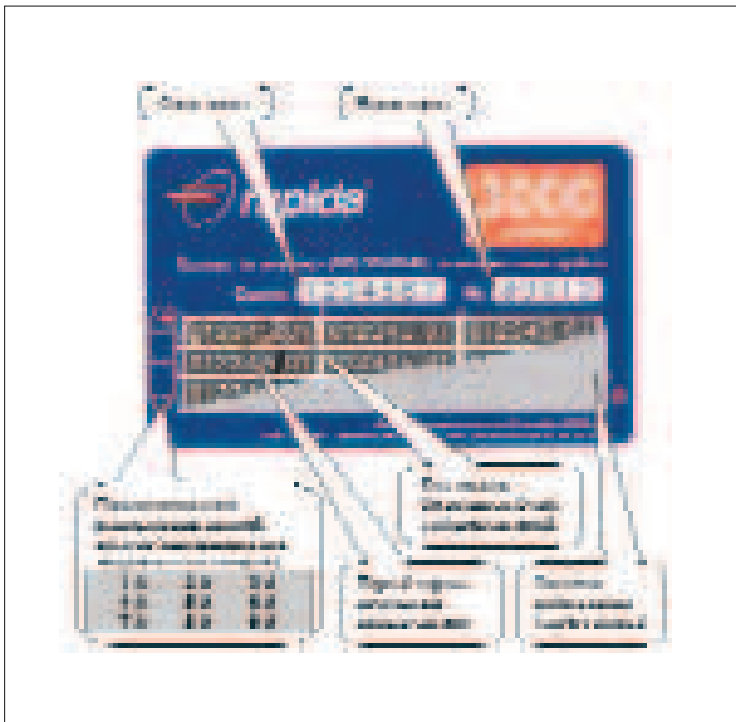
ИЗ-ЗА ТОГО, ЧТО DES ПРОДЕМОНСТРИРОВАЛ МАССУ СВОИХ НЕДОСТАТКОВ, ИСПОЛЬЗУЕТСЯ ЕГО ВАРИАЦИЯ — РЕЖИМ 3DES, КОТОРЫЙ МОЖЕТ ИСПОЛЬЗОВАТЬ ДВА ИЛИ ТРИ КЛЮЧА. РЕЖИМ ЗАШИФРОВАНИЯ НА 3 КЛЮЧАХ (168 БИТ КЛЮЧА И 112 ЭФФЕКТИВНЫХ БИТ): $C = E(K_3, E(K_2, E(K_1, M)))$. ГДЕ C — КРИПТОТЕКСТ, M — ОТКРЫТЫЙ ТЕКСТ, K_1 — КЛЮЧИ, E- РЕЖИМ ЗАШИФРОВАНИЯ. РАСШИФРОВАНИЕ ПРОИЗВОДИТСЯ В ОБРАТНОМ ПОРЯДКЕ: $M = D(K_1, D(K_2, D(K_3, C)))$. С АНАЛОГИЧНОЙ СТОЙКОСТЬЮ МОЖНО ИСПОЛЬЗОВАТЬ ВСЕГО ДВА КЛЮЧА (112 ЭФФЕКТИВНЫХ БИТ КЛЮЧА). СХЕМА ВЫГЛЯДИТ СЛЕДУЮЩИМ ОБРАЗОМ. РЕЖИМ ЗАШИФРОВАНИЯ: $C = E(K_1, D(K_2, E(K_1, M)))$; РАСШИФРОВАНИЯ: $M = D(K_1, E(K_2, D(K_1, C)))$. ЕДИНСТВЕННОЕ ОГРАНИЧЕНИЕ НА ИСПОЛЬЗОВАНИЕ ЭТИХ РЕЖИМОВ (ВПРОЧЕМ, КАК И ДЛЯ ОДНОРАЗОВОГО ИСПОЛЬЗОВАНИЯ) — ЭТО ПРОВЕРКА ИСПОЛЬЗУЕМЫХ КЛЮЧЕЙ НА ВЫРОЖДЕННОСТЬ ИЛИ ПОЛУВЫРОЖДЕННОСТЬ.

ОДНАКО ВСЕ ЭТИ КЛЮЧИ ИЗВЕСТНЫ, И ДОСТАТОЧНО СДЕЛАТЬ ВСЕГО НЕСКОЛЬКО ДОПОЛНИТЕЛЬНЫХ ПРОВЕРОК ПРИ ФОРМИРОВАНИИ КЛЮЧЕЙ. ДЛЯ ЗАШИФРОВАНИЯ И РАСШИФРОВАНИЯ ИСПОЛЬЗУЮТСЯ ОДНИ И ТЕ ЖЕ КЛЮЧИ. ВОТ ПОЧЕМУ ДЛЯ ПРИМЕНЕНИЯ СИММЕТРИЧНЫХ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ КРИТИЧНЫМ ЯВЛЯЕТСЯ ЗАЩИЩЕННЫЙ КАНАЛ ПЕРЕДАЧИ КЛЮЧЕЙ, ПОСКОЛЬКУ ИХ ДИСКРЕДИТАЦИЯ ПРИВОДИТ К ДИСКРЕДИТАЦИИ ВСЕХ (!) СООБЩЕНИЙ, ЗАЩИЩЕННЫХ ЭТИМИ КЛЮЧАМИ. ПРИ ЭТОМ ВВОД В ДЕЙСТВИЕ КЛЮЧЕЙ ДОЛЖЕН БЫТЬ ОДНОВРЕМЕННЫМ НА ОБОИХ КОНЦАХ ЗАЩИЩАЕМОГО КАНАЛА.

ВТОРАЯ СЛОЖНОСТЬ ПРИ ИСПОЛЬЗОВАНИИ СИММЕТРИЧНЫХ АЛГОРИТМОВ В ОБЩЕМ СЛУЧАЕ — ЭТО НЕОБХОДИМОСТЬ ИМЕТЬ МНОЖЕСТВО КЛЮЧЕЙ. ДЕЙСТВИТЕЛЬНО, ИСПОЛЬЗОВАНИЕ ЕДИНСТВЕННОГО КЛЮЧА ДЛЯ ВСЕХ АБОНЕНТОВ СЕТИ ПОЗВОЛЯЕТ КАЖДОМУ АБОНЕНТУ ЧИТАТЬ ВСЕ СООБЩЕНИЯ, А ПРИ УВЕЛИЧЕНИИ МЕЖАБОНЕНТСКИХ СВЯЗЕЙ ЧИСЛО КЛЮЧЕЙ РАСТЕТ В ГЕОМЕТРИЧЕСКОЙ ПРОГРЕССИИ (ПРОБЛЕМА ДОСТАВКИ КЛЮЧЕЙ).

но улучшить финансовое положение мошенника. А ты вспомнил бы, за что заплатил три доллара два месяца назад?

Депозитные карты — не такая легкая нажива, так как для доступа к их использованию на POS-терминале требуется ввести PIN-код (personal identify number) или в онлайн получить код подтверждения операции от процессинга. Тут мошенник обязательно пытается посмотреть код, без которого знание реквизитов карты бесполезно — вот такими сложными махинациями увлекаются немногие. Еще одна причина непопулярности депозитных карт среди преступников — невозможность перебора даже несмотря на то, что PIN-код карт содержит всего четыре цифры. Как правило, после третьей попытки неверного набора PIN'a карта блокируется и изымается банкоматом или продавцом. Более сложный случай — преступный сговор владельца карты и обслуживающего персонала. После «двойной прокатки» продавец отменяет транзакцию и возвращает деньги клиенту, а потом оба делят добычу. Плюс владелец карты получает оплаченные транзакцией товар или услугу.



Точка обслуживания пластиковых карт без продавца — это в 99% случаев банкомат (АТМ). С точки зрения мошенника, банкомат — почти идеальное место для обналичивания денег, сбора информации, подготовки банальной кражи банковских карт. Кстати, многие зря хранят банковские карты в конверте с PIN-кодом, тем самым сильно упрощая жизнь ворам.

Банкомат привлекателен для преступников и как источник самых разных способов сбора информации. В начале 90-х годов XX века некие деятели в США собрали три банкомата, которые были очень похожи на настоящие, только не выдавали денег, а вместо этого снимали данные с карты и запоминали соответствующий PIN-код, затем сообщали честному владельцу карты, что в кассете закончились деньги. Ситуация обычна для банкоматов, и разочарованные граждане, не подозревая дурного, шли искать другой агрегат. В течение нескольких недель эти фальшивки ко-

ОСНОВНОЙ СПОСОБ МОШЕННИЧЕСТВА — КОЛДОВОСТВО С ЧУЖИМИ ИДЕНТИФИКАЦИОННЫМИ ДАННЫМИ.

алгоритмы для хэшей

АЛГОРИТМОВ КРИПТОГРАФИЧЕСКИХ ХЭШЕЙ ДОВОЛЬНО МНОГО, НО БОЛЬШЕ ВСЕГО РАСПРОСТРАНИЛСЯ ЗА ПОСЛЕДНИЕ ГОДЫ АЛГОРИТМ MD5 (MESSAGE DIGEST), РАЗРАБОТАННЫЙ АМЕРИКАНСКОЙ КОМПАНИЕЙ RSA DATA SECURITY ИЗ КЛАССА MDС. УВЫ, В НАЧАЛЕ ЭТОГО ГОДА В ЭТОМ АЛГОРИТМЕ СНАЧАЛА КИТАЙСКИЕ, А ЗАТЕМ ЧЕШСКИЕ СПЕЦИАЛИСТЫ ОБНАРУЖИЛИ СЕРЬЕЗНУЮ СЛАБОСТЬ, КОТОРАЯ ПРИВОДИТ К НАХОЖДЕНИЮ КОЛЛИЗИИ ЗА 6-40 ЧАСОВ. ОДНАКО АКТУАЛЬНОСТЬ ИНФОРМАЦИИ ПРИ ОБМЕНЕ БАНКОМАТА ИЛИ POS-ТЕРМИНАЛА С ПРОЦЕССИНГОМ СОСТАВЛЯЕТ МАКСИМУМ НЕСКОЛЬКО ДЕСЯТКОВ СЕКУНД, ПОЭТОМУ НЕ СТОИТ ОСОБО ВОЛНОВАТЬСЯ ЗА ПОДОБНУЮ АТАКУ, ХОТЯ СИСТЕМАМ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ПРИДЕТСЯ ТУГО. НЕ ИСКЛЮЧЕНО, ЧТО АМЕРИКАНСКИЕ СПЕЦИАЛИСТЫ ЗНАЛИ О ВОЗМОЖНОСТИ ТАКОЙ АТАКИ, ПОСКОЛЬКУ В КАЧЕСТВЕ НАЦИОНАЛЬНОГО СТАНДАРТА БЫЛ ПРИНЯТ ДРУГОЙ АЛГОРИТМ — SHA (SECURE HASH STANDARD), РАЗРАБОТАННЫЙ NIST — NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (FIP-180 — FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 180). ПОСЛЕДНИЙ ВАРИАНТ СТАНДАРТА (SHA-1) БЫЛ ВВЕДЕН В ДЕЙСТВИЕ В 1994 ГОДУ ДОКУМЕНТОМ FIPS PUB 180-1, SECURE HASH STANDARD, 1994.

отпор мошенникам

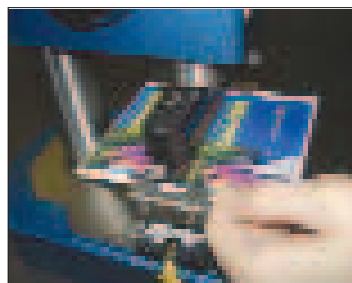
ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ С ПЛАСТИКОВЫМИ КАРТАМИ ОСУЩЕСТВЛЯЕТСЯ НЕ ТОЛЬКО И НЕ СТОЛЬКО ТЕХНИЧЕСКИМИ СРЕДСТВАМИ, А ЦЕЛЫМ КОМПЛЕКСОМ МЕР: ОРГАНИЗАЦИОННЫЕ МЕРЫ, В ТОМ ЧИСЛЕ ПРАВИЛА ВЫДАЧИ КАРТЫ КЛИЕНТУ И ЕЕ ИСПОЛЬЗОВАНИЯ, ПРАВИЛА ПРИЕМА И ПРОВЕРКИ ВАЛИДНОСТИ КАРТЫ В ТОЧКЕ ОБСЛУЖИВАНИЯ, ПРЕДУПРЕЖДЕНИЕ БАНКАМИ МОШЕННИЧЕСТВ В ТОЧКАХ ОБСЛУЖИВАНИЯ, ПРИВЕДЕНИЕ ПРАВИЛ МПС (МЕЖДУНАРОДНЫХ ПЛАТЕЖНЫХ СИСТЕМ) В СООТВЕТСТВИИ С ПРАВОВЫМИ НОРМАМИ СТРАНЫ И Т.П. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ВЫСТУПАЮТ НА СЦЕНУ ТОЛЬКО ЕСЛИ КЛИЕНТ ПЫТАЕТСЯ ПОЛУЧИТЬ ДОСТУП К УСЛУГЕ ПРИ ПОМОЩИ КАРТЫ.

чевали по городу (кажется, по Нью-Йорку), а затем мошенники начали ураганно потрошить счета, используя собранные данные. Места обналичивания, банки и процессинги, ставшие жертвами мошенников, были разные; среди огромной массы одинаковых транзакций с совершенно правильными данными засечь случаи краж было сложно, поэтому преступление долго не обнаруживалось.

Оперативники ФБР нашли и похитителей, и фальшивые аппараты, не нашли только деньги. Ценный опыт этого дела был творчески переосмыслен, развит и в дальнейшем перенесен в другие страны и континенты. Например, в прошлом году в Москве была обнаружена и арестована группа лиц (в основном из студентов), которые устанавливали на реальные действующие банкоматы на вход в картоприемник специальную насадку и миниатюрную камеру. Когда проводились совершенно легальные операции по снятию денег или оплате счетов, насадка считывала данные с магнитной полосы, а видеокамера записывала, если удавалось, набор PIN-кода. Далее на заранее заготовленные имитаторы карт (повторять защитные признаки карт не было необходимости, так как АТМ не может проверить их) заносилась необходимая информация и счета «потрошились» с фантастической скоростью. Маловероятно, чтобы человек, который только что провел операцию на банкомате, в ближайшее время подошел бы к нему снова с картой, поэтому у мошенников было достаточно времени. За несколько месяцев напряженного труда мошенники сняли несколько сотен тысяч долларов, но скоро были арестованы. Открытая печать не сообщала, попала ли «под раздачу» вся преступная группа, но эксперты высоко оценили технический уровень использованных ими приборов.

Более экзотический и грубый случай — физическое выдирание банкомата трактором или грузовиком и дальнейшее изъятие в тихом месте кассет с деньгами. Его не рассматриваем, он ничем не отличается от грабежа банка. Это занятие для медвежатников (АТМ — фактически сейф), а не для приличных людей вроде нас :).

Еще одно вероятное направление атаки — связь POS-терминала или АТМ с процессинговым центром. Если возможно



внедриться в канал связи и раскрыть некоторую секретную информацию данного банкомата или терминала, от его лица можно посылать в процессинг транзакции, которые будут признаны истинными. Справедливо и наоборот.

Самая очевидная атака — запросить с поддельной карты некоторую сумму, а в результате подменить отрицательный ответ процессинга и получить деньги. Ход очевидный, но не без загвоздок. Канал защищен при помощи криптографических алгоритмов. Обычно используется симметричный алгоритм DES (Data Encryption Standard) или его клон 3DES.

В ряде случаев используется не тотальное шифрование сообщения в процессинг и квитанции процессинга в банкомат, как можно было бы ожидать, а лишь подпись транзакции с использованием секретного ключа. Такой режим называется MAC (Message Authentication Code), и он является вариантом электронной подписи с использованием секретного ключа. Суть MAC в том, что шифруется не все сообщение, а только хэш (дайджест или свертка) от него. Такая свертка называется криптографическим хэшем.

Другие возможные атаки на платежные системы направлены на сам банк-эмитент или процессинговый центр. К счастью, подобные атаки практически невозможны. Дело в том, что технология прохождения транзакции от точки обслуживания не предполагает взаимодействия с операционным днем банка и не имеет доступа к банковским счетам. Более того, карта имеет свой ежедневный лимит доступа к сумме счета, которую банк-эмитент определяет и ежедневно сообщает в процессинг. Таким образом, банк не имеет возможности работать с банкоматом напрямую, а банкомат — с банком. Процессинговый центр же понятия не имеет о реальном состоянии счета. Так что и работники этих кредитных организаций имеют доступ к информации в рамках своей компетенции. Например, работник процессингового центра не сможет получить реальные PIN-коды, так как они хранятся в специальных хранилищах, притом не в реальном виде, а в виде хэша.

Разумеется, это не исключает инсайдерских атак (совершенных работниками банка внутри охраняемого периметра). Как правило, такие атаки связаны не с технической защищенностью системы пластиковых карт, а с «дырами» в организации ее работы. Например, однажды уволенный администратор смог воспользоваться своими правами (которые должны были быть отменены в момент увольнения) с консоли внутри ЛВС банка (почему его вообще допустили до рабочего места?).

Атака была обнаружена в момент завершения операционного дня банка, и следующие два дня служба безопасности работала в особо насыщенном режиме — ловили мошенника. К сожалению, не всегда это удается. Известен случай в Санкт-Петербурге, когда атака вполне удалась и виновного задержать не удалось.

ДЛЯ КРЕДИТНЫХ КАРТ МОШЕННИКИ ПРАКТИКУЮТ «ДВОЙНУЮ ПРОКАТКУ».

ПРОТИВОДЕЙСТВИЕ МОШЕННИЧЕСТВУ СОСТОИТ ИЗ ЦЕЛОГО КОМПЛЕКСА МЕР.

АЛГОРИТМОВ КРИПТОГРАФИЧЕСКИХ ХЭШЕЙ МНОГО, НО НАИБОЛЬШЕЕ РАСПРОСТРАНЕНИЕ ПОЛУЧИЛ АЛГОРИТМ MD5.



Что такое ХЭШ

ХЭШ — ЭТО ПРЕОБРАЗОВАНИЕ, ПОЛУЧАЮЩЕЕ ИЗ ДАННЫХ ПРОИЗВОЛЬНОЙ ДЛИНЫ НЕКОЕ ЗНАЧЕНИЕ (СВЕРТКУ) ФИКСИРОВАННОЙ ДЛИНЫ. ПРОСТЕЙШИМИ ПРИМЕРАМИ ЯВЛЯЮТСЯ КОНТРОЛЬНЫЕ СУММЫ (НАПРИМЕР CRC32).

БЫВАЮТ КРИПТОГРАФИЧЕСКИЕ И ПРОГРАММИСТСКИЕ ХЭШИ. КРИПТОГРАФИЧЕСКИЙ ХЭШ ОТЛИЧАЕТСЯ ОТ ПРОГРАММИСТСКОГО ДВУМЯ СВОЙСТВАМИ: НЕОБРАТИМОСТЬЮ И СВОБОДНОСТЬЮ ОТ КОЛЛИЗИЙ. ОБОЗНАЧИМ: М — ИСХОДНЫЕ ДАННЫЕ, Н(М) — ХЭШ ОТ НИХ. НЕОБРАТИМОСТЬ ОЗНАЧАЕТ, ЧТО ЕСЛИ ИЗВЕСТНО ЧИСЛО НО, ТО ТРУДНО ПОДОБРАТЬ М ТАКОЕ, ЧТО Н(М) = НО. СВОБОДНОСТЬ ОТ КОЛЛИЗИЙ ОЗНАЧАЕТ, ЧТО ТРУДНО ПОДОБРАТЬ ТАКИЕ М1 И М2, ЧТО М1 ≠ М2, НО Н(М1) = Н(М2).

криптографические хэш-функции разделяются на два класса:

- 1 ХЭШ-ФУНКЦИИ БЕЗ КЛЮЧА, MDC-КОДЫ (MODIFICATION/MANIPULATION DETECT CODE);
- 2 ХЭШ-ФУНКЦИИ С КЛЮЧОМ, MAC-КОДЫ (MESSAGE AUTHENTICATION CODE).

хэш-функции без ключа разделяются на два подкласса:

- 1 СЛАБЫЕ ХЭШ-ФУНКЦИИ;
- 2 СИЛЬНЫЕ ХЭШ-ФУНКЦИИ.

СЛАБОЙ ХЭШ-ФУНКЦИЕЙ НАЗЫВАЕТСЯ ОДНОСТОРОННЯЯ ФУНКЦИЯ Н(Х), КОТОРАЯ УДОВЛЕТВОРЯЕТ СЛЕДУЮЩИМ УСЛОВИЯМ:

- 1 АРГУМЕНТ Х МОЖЕТ БЫТЬ СТРОКОЙ БИТ ПРОИЗВОЛЬНОЙ ДЛИНЫ;
- 2 ЗНАЧЕНИЕ Н(Х) ДОЛЖНО БЫТЬ СТРОКОЙ БИТ ФИКСИРОВАННОЙ ДЛИНЫ;
- 3 ЗНАЧЕНИЕ Н(Х) ЛЕГКО ВЫЧИСЛИТЬ;
- 4 ДЛЯ ЛЮБОГО ФИКСИРОВАННОГО Х ВЫЧИСЛИТЕЛЬНО НЕВОЗМОЖНО НАЙТИ ДРУГОЙ Х' ≠ Х, ТАКОЙ ЧТО Н(Х')=Н(Х); ПАРА Х' ≠ Х, КОГДА Н(Х')=Н(Х), НАЗЫВАЕТСЯ КОЛЛИЗИЕЙ ХЭШ-ФУНКЦИИ;

СИЛЬНОЙ ХЭШ-ФУНКЦИЕЙ НАЗЫВАЕТСЯ ОДНОСТОРОННЯЯ ФУНКЦИЯ Н(Х), КОТОРАЯ УДОВЛЕТВОРЯЕТ УСЛОВИЯМ 1-3 ДЛЯ СЛАБОЙ ХЭШ-ФУНКЦИИ И СВОЙСТВУ:

- 5 ВЫЧИСЛИТЕЛЬНО НЕВОЗМОЖНО НАЙТИ ЛЮБУЮ ПАРУ Х' ≠ Х, ТАКОЙ ЧТО Н(Х')=Н(Х).

ПОСКОЛЬКУ ИЗ СВОЙСТВ 1-2 СЛЕДУЕТ, ЧТО МНОЖЕСТВО ОПРЕДЕЛЕНИЯ ХЭШ-ФУНКЦИИ ЗНАЧИТЕЛЬНО ШИРЕ МНОЖЕСТВА ЗНАЧЕНИЙ, ТО КОЛЛИЗИИ ДОЛЖНЫ СУЩЕСТВОВАТЬ. СВОЙСТВО 4 ТРЕБУЕТ, ЧТОБЫ НАЙТИ ИХ ДЛЯ ЗАДАННОГО ЗНАЧЕНИЯ Х БЫЛО ПРАКТИЧЕСКИ НЕВОЗМОЖНО. ТРЕБОВАНИЕ 4' ГОВОРIT О ТОМ, ЧТО У СИЛЬНОЙ ХЭШ-ФУНКЦИИ ВЫЧИСЛИТЕЛЬНО НЕВОЗМОЖНО НАЙТИ КАКУЮ-ЛИБО КОЛЛИЗИЮ.

ХЭШ-ФУНКЦИЕЙ С КЛЮЧОМ (MAC) НАЗЫВАЕТСЯ ФУНКЦИЯ Н(К,Х), УДОВЛЕТВОРЯЮЩАЯ СВОЙСТВАМ:

- 1 АРГУМЕНТ Х ФУНКЦИИ Н(К,Х) МОЖЕТ БЫТЬ СТРОКОЙ БИТ ПРОИЗВОЛЬНОЙ ДЛИНЫ;
- 2 ЗНАЧЕНИЕ Н(К,Х) ДОЛЖНО БЫТЬ СТРОКОЙ БИТ ФИКСИРОВАННОЙ ДЛИНЫ;
- 3 ПРИ ЛЮБЫХ К И Х ЛЕГКО ВЫЧИСЛИТЬ Н(К,Х);
- 4 ДЛЯ ЛЮБОГО Х ДОЛЖНО БЫТЬ ТРУДНО ВЫЧИСЛИТЬ Н(К,Х), НЕ ЗНАЯ К;
- 5 ДОЛЖНО БЫТЬ ТРУДНО ОПРЕДЕЛИТЬ К ДАЖЕ ПРИ БОЛЬШОМ ЧИСЛЕ НЕИЗВЕСТНЫХ ПАР {Х, Н(К,Х)} ПРИ ВЫБРАННОМ НАБОРЕ Х ИЛИ ВЫЧИСЛИТЬ ПО ЭТОЙ ИНФОРМАЦИИ Н(К,Х') ДЛЯ Х' ≠ Х.

Виртуальный метаболизм

КАК ВЫВЕСТИ СВОЮ НАЛИЧНОСТЬ ИЛИ ПОЛОЖИТЬ ЕЕ НА СЧЕТ — ВСЕ ДОСТУПНЫЕ СПОСОБЫ И ИХ БЕЗОПАСНОСТЬ

ВОПРОС ОБ ОБМЕНЕ ВИРТУАЛЬНЫХ ДЕНЕГ СТАНОВИТСЯ ВСЕ БОЛЕЕ АКТУАЛЬНЫМ. НА ДАННЫЙ МОМЕНТ СУЩЕСТВУЕТ НЕСКОЛЬКО СПОСОБОВ ОБМЕНА Е-ВАЛЮТЫ. РАЗБЕРЕМСЯ, ЧТО ЭФФЕКТИВНЕЕ И БЕЗОПАСНЕЕ | **КРУПИНОВ АНТОН АКА RELIFE FEAT SATURN (ANTMIXION@MAIL.RU)**



Электронные платежи (электронные деньги) обретают все большую популярность, их количество растет в геометрической прогрессии. Существующие платежные системы (E-gold, WebMoney, PayPal, Stormpay, RuPay, «Яндекс.Деньги», «Рапида») позволяют не только приобрести практически любой товар или услугу в интернете, но и получать зарплату в «цифровых деньгах», если, например, работодатель находится не в твоём городе или не в твоей стране. А как же обмен одной виртуальной валюты в другую, перевод честно заработанного в бумажные деньги, чтобы и руками потрогать, и к сердцу прижать :)? Для этих целей (обмен между различными платежными системами, ввод-вывод денег) и созданы электронные обменные центры.

обмен Конвертирование валютных единиц одной системы в другие (например E-gold в WebMoney) осуществляется в любом из автоматических обменных пунктов.

roboxchange Один из первых в рунете автоматических обменных пунктов. Надежный, имеет большие денежные резервы, однако берет достаточно большую комиссию (около 3%). Кроме обмена, Robo предоставляет и другие услуги: покупка «игровых денег», вывод «игровых денег», перевод электронных денег на карточку, оплата мобильного телефона, спутникового телевидения и интернет-услуг.

exchange.net.ua Украинский обменный пункт, один из лучших автоматических обменников. Возможен обмен практически всех существующих интернет-денег. Есть выгодная партнерская программа.

expert exchange! Обменный пункт в США (Нью-Йорк). Поддерживает обмен: PayPal, E-Gold, WebMoney, Yandex, iKobo, Western Union и другие менее популярные. Работает с аукционом eBay при продаже или покупке, можно установить прием платежей PayPal и на собственном сайте. Конечно же, имеется аттестат Регистратора в системе Webmoney Transfer.

ppwm.com Автоматический обменник в Германии (Нюрнберг). Производит переводы из PayPal в Webmoney и наоборот.

В абсолютном большинстве случаев операция обмена выполняется через web-интерфейс по стандартному защищенному соединению. Механизм

ПРИ ВЫВОДЕ ДЕНЕГ ИЗ СИСТЕМЫ ГАРАНТИИ ОТСУТСТВУЮТ, ТАК КАК НЕ ЗАКЛЮЧАЕТСЯ НИКАКОГО ДОГОВОРА НА УСЛУГУ

обмена прост, как топор: отправляешь деньги в одной валюте, получаешь в другой, «из тебя» вычитают комиссию (в среднем 1-2%). Кроме автоматических пунктов, которые занимаются только конвертацией валют, существуют центры, в которых можно положить деньги на счет платежной системы или снять их со счета.

ВВОД-ВЫВОД Идея этого процесса следующая. Ты доверяешь свои реальные (или электронные) деньги обменнику, который обязуется перевести их в электронные (реальные). Однако для того чтобы схема заработала, организатору центра приема платежей нужно заручиться поддержкой — обычно это договор между банком (или другой финансовой организацией) и платежной системой. Договор предусматривает операции с очень низким процентом комиссии. Существуют схемы, при которых банки сами эмитируют электронную наличность.

Самая популярная система в России — WebMoney Transfer, на ее примере и рассмотрим все доступные способы ввода и вывода денег.

Способы ввода:

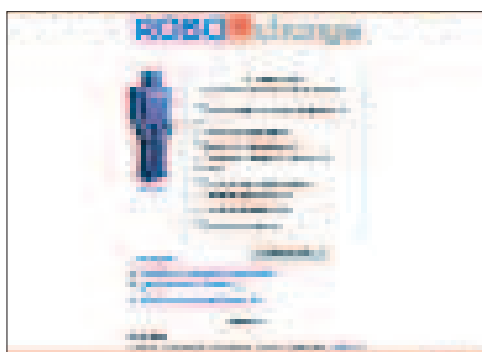
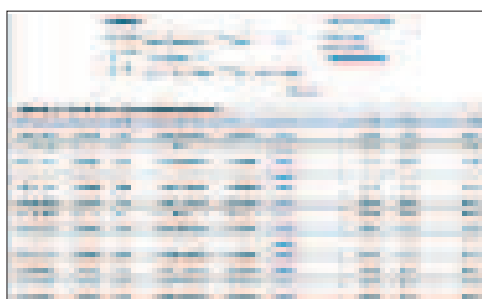
- 1 БАНКОВСКИЙ ПЕРЕВОД;
- 2 ЗАЧИСЛЕНИЕ С ПОМОЩЬЮ WM-КАРТЫ;
- 3 ОБМЕН НАЛИЧНЫХ (БЕЗНАЛИЧНЫХ) НА WM В ОДНОЙ ИЗ СЕКЦИЙ БИРЖИ — www.exchanger.ru;
- 4 ОБМЕН НАЛИЧНЫХ НА WM В ОДНОМ ИЗ ОБМЕННЫХ ПУНКТОВ;
- 5 ОБМЕН ЭЛЕКТРОННОЙ ВАЛЮТЫ ДРУГИХ СИСТЕМ;
- 6 ПОЧТОВЫЙ ПЕРЕВОД ЧЕРЕЗ СИСТЕМУ ELPAY;
- 7 НАЛИЧНЫМИ В БАНКАХ И ПУНКТАХ ПРИЕМА;
- 8 НАЛИЧНЫМИ В АВТОМАТАХ И БАНКОМАТАХ;
- 9 ЗАЧИСЛЕНИЕ ЧЕРЕЗ SMS.

Способы вывода:

- 1 БАНКОВСКИЙ ПЕРЕВОД;
- 2 ПЕРЕВОД WMZ НА БАНКОВСКУЮ ПЛАТЕЖНУЮ КАРТУ СЕРВИСА «ПЛАТЕЖНЫЕ КАРТЫ + WEBMONEY»;
- 3 ОБМЕН WM НА НАЛИЧНЫЕ (БЕЗНАЛИЧНЫЕ) В ОДНОЙ ИЗ СЕКЦИЙ БИРЖИ www.exchanger.ru;
- 4 ОБМЕН WM НА НАЛИЧНЫЕ В ОДНОМ ИЗ ОБМЕННЫХ ПУНКТОВ;
- 5 ОБМЕН WM НА ЭЛЕКТРОННУЮ ВАЛЮТУ ДРУГИХ СИСТЕМ;
- 6 ОБМЕН WMZ НА USD С ПЕРЕВОДОМ ЧЕРЕЗ WESTERN UNION;
- 7 ОБМЕН WMR НА РОССИЙСКИЕ РУБЛИ ПОЧТОВЫМ ПЕРЕВОДОМ.

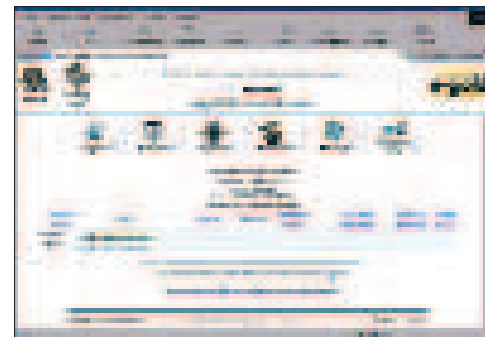
Некоторые варианты ввода-вывода возможны или невозможны в зависимости от того, какая электронная валюта (WMZ, WMR, WME, WMU) вводится или какая реальная валюта выводится (USD, RUR, EUR, UAH). К примеру, способы ввода WMZ ограничиваются только пунктами с первого по пятый.

Все эти варианты далеко не равноценны по сроку выполнения, и если в одном случае перечисление происходит мгновенно, то в другом придется ждать день, два, неделю. Ясно, что, например, почтовый пе-



ИНОГДА
КОНФИДЕНЦИАЛЬНОСТЬ ВАЖНЕЕ,
ЧЕМ ПРОЦЕНТ ЗА
ОБНАЛИЧКУ

ЗАЩИТА ПЛАТЕЖНЫХ СИСТЕМ ДОСТАТОЧНО КРЕПКАЯ, ПОЭТОМУ ЕЕ ПРОБИВАЮТ, КАК ПРАВИЛО, СОЦИАЛЬНОЙ ИНЖЕНЕРИЕЙ



Интерфейс к
аккаунту в E-gold

ревод по времени затянется намного больше, чем непосредственный обмен в одном из обменных пунктов.

Оптимальным способом ввода (не требуется заполнять никакие документы, подписывать договоры и т.п.) стало зачисление денег при помощи SMS — этот сервис не был предусмотрен изначально, но постепенно завоевал популярность.

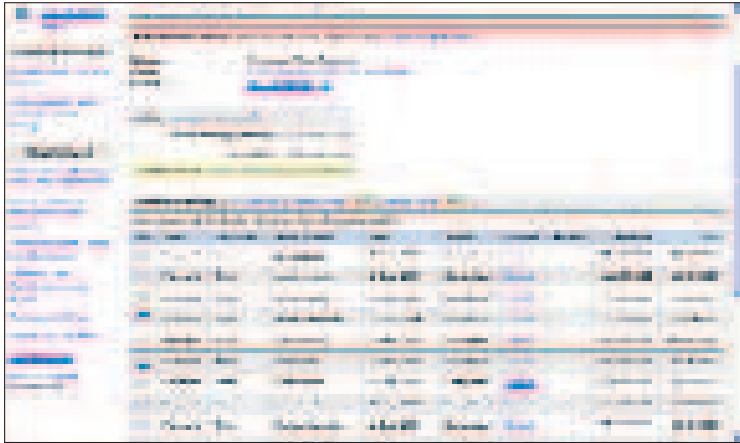
Что касается вывода средств из системы, то здесь нет универсального способа, как при вводе. В качестве более-менее удобного способа предлагают перевод WMZ на банковскую платежную карту сервиса «Платежные карты + WebMoney». Выдача платежных карт клиентам WebMoney Transfer производится совместно с банками — участниками МПС (Visa, Eurocard/Mastercard и др.). Сервис закрепляет каждую выдаваемую карту за определенным WM-идентификатором участника системы, поэтому владелец может быстро и не прибегая к дорогим банковским переводам перебрасывать деньги с WM-кошелька на карту. В дальнейшем деньги с карты можно будет получить в любом из многочисленных банкоматов, расплачиваться средствами с карты за товары и услуги в магазинах и компаниях, которые принимают банковские платежные карты. Один раз потратил время, получил карту — и больше не раздумываешь, как вывести свои деньги поудобнее. Смущает одно: этот сервис доступен только для WMZ.

АНОНИМНЫЙ ВЫВОД Обналичивание средств (особенно добытых не совсем честным путем) через обменные пункты — процедура, которая, как правило, требует удостоверения личности. Однако бывают ситуации, когда идентификация очень нежелательна. Именно для сохранения статуса инкогнито в Сети предусмотрены интернет-банки. Считается, что в этой сфере услуг хорошо зарекомендовали себя www.fethard.biz (Россия) и www.yambo.biz (Великобритания) — открытие виртуального счета займет всего несколько минут, после этого ты сразу сможешь выполнять нужные операции (например безналичные переводы средств из другого банка). При регистрации не требуют никаких документов, так что анонимность гарантирована.

Для пополнения счета с помощью электронных денег потребуется заказать их перевод из электронных платежных систем. При получении на свой счет безналичных платежей такие банки используют единые для всех клиентов банковский счет и банковские реквизиты. А чтобы перевод нашел своего получателя, в строке «Назначение платежа» отправитель указывает «Платеж для клиента номер ...».

Для ввода электронных средств через интернет-банк комиссия колеблется в районе 1%. После перехода денег на твой виртуальный счет в интернет-банке ты можешь сделать с ними все, что пожелаешь (естественно, в пределах тех услуг, которые предлагает данный конкретный сервис). Получить деньги через Western Union, перевести их в другой банк (в том числе другому лицу), сконвертировать их в какую-либо электронную валюту и т.д. Стало популярно переводить деньги на так называемую анонимную банковскую карту и потом снимать с нее наличные.

сверху вниз:
История денежных
телодвижений
Виртуальный
обменник
RoboXChange



Наглядный пример
аккаунта в системе
PayPal

Едва ли не единственный минус вывода денег через интернет-банк — отсутствие внятных гарантий со стороны банка. Договор об обслуживании не заключается, соответственно, банк не несет никаких обязательств.

безопасность Надежность обменных пунктов в основном зависит от используемых ими платежных систем. Именно в этом звене, как правило, и кроются уязвимые места, так как весь механизм обмена сводится к следующему: из своего кошелька клиент перечисляет некоторую электронную сумму на кошелек продавца услуг; тот удостоверяется, пришла ли сумма на счет, затем оказывает оговоренную услугу (обменивает деньги на другую электронную валюту или выводит их наличными).

В платежной системе WebMoney Transfer деньги представляют собой совокупность записей по произведенным транзакциям. В другом случае е-валюты — это определенный буквенно-цифровой код, который система воспринимает как купюру конкретного достоинства. При получении такого кода злоумышленник сможет создать себе некоторое количество денег — вот и халява! С другой стороны, это свойство е-валюты имеет большой и жирный плюс — возможность получить деньги в виде электронной наличности на предъявителя.

механизмы защиты При заключении сделки в интернете покупатель и продавец находятся в онлайн, поэтому совершенно закономерно, что при проведении транзакции платежные системы, использующие электронные средства оплаты, связываются с авторизационным центром, чтобы идентифицировать клиента и подтвердить его платежеспособность.

Для обеспечения безопасности транзакций система WebMoney использует несколько защитных механизмов, завязанных в комплекс:

- 1 ОПЕРАЦИИ (РАСЧЕТЫ МЕЖДУ УЧАСТНИКАМИ, ВЫПИСКА СЧЕТОВ, ОБМЕН СООБЩЕНИЯМИ) ПРОВОДЯТСЯ В ЗАКОДИРОВАННОМ ВИДЕ НА ОСНОВЕ АЛГОРИТМА ШИФРОВАНИЯ С ДЛИНОЙ КЛЮЧА 1040 БИТ, ПОДОБНОГО RSA.
- 2 ЧТОБЫ ОБЕСПЕЧИТЬ АБСОЛЮТНУЮ КОНФИДЕНЦИАЛЬНОСТЬ СДЕЛОК, ПРИ КАЖДОМ СЕАНСЕ ГЕНЕРИРУЮТСЯ УНИКАЛЬНЫЕ СЕАНСОВЫЕ КЛЮЧИ.

Безопасность системы «Яндекс.Деньги» опирается на криптографический алгоритм RSA с длиной ключа 1024 бит. Каждая финансовая операция заверяется подписью процессингового центра системы, а сообщения шифруются и подписываются с помощью ПО отправляющей стороны.

Довольно эффективная защита. Так что на вооружении е-money-грабителей остаются лишь методы социальной инженерии либо перехват реквизи-

тов с помощью троянов, кейлоггеров и т.п. Чтобы пользователь добровольно скачал себе троян, придумывают массу разных «интересных предложений» — от надоевшего всем генератора WM до всяческих рабочих приложений, в которые вшит троян. Если жертва заражена успешно, хакер получает всю (или отфильтрованную) информацию, в том числе ключи, аккаунты и проч. Но впереди хакера ожидают другие проблемы...

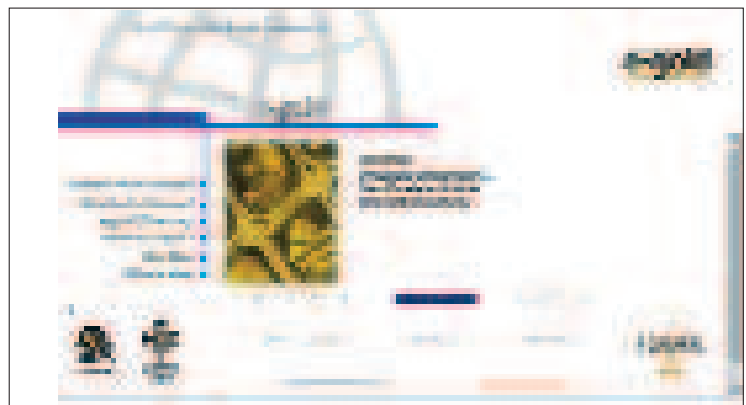
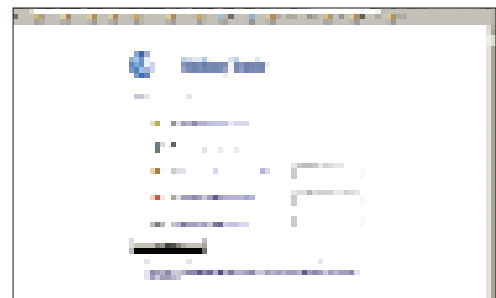
Эти платежные системы значительно отличаются от систем управления счетом, при взломе которых достаточно перехватить ключевую информацию (номер кредитной карты и т.п.) — это и есть доступ к счету. Поэтому, например, для хакающего «Яндекс.Деньги» получение и расшифровка информации — только полдела, а вторая половина — это вскрытие добытых ключей. Разоблачить ключ длиной 1024 бита в разумные сроки практически нереально, так что нужно охотиться за незашифрованными данными.

Для пользователей можно выдвинуть предложение: «Пришли на такой-то кошелек такую-то сумму и тут же получишь взамен сумму в два раза больше!» Самое удивительное, что многие откликаются на просьбы :), особенно если ты не забираешь деньги сразу, а завлекаешь дальше, действительно переводя клиенту нужную сумму.

Обмен валюты тоже не обходится без мошенников. Оригинальный способ заполучить деньги у доверчивых пользователей — создать фальшивые обменные пункты, в которых предлагается обменять одну электронную валюту на другую по заманчивому курсу. Но для начала выгодного обмена от пользователя требуют скачать и установить специальную программу, под которой скрывается троян, с помощью которого и опустошается кошелек жертвы.

Появление электронных обменных центров закономерно, их «породил» активный оборот электронных денег на просторах всемирной паутины. Обменники появились сравнительно недавно, поэтому их использование затруднено, а механизмы обмена недостаточно проработаны. Но как все новое и стремительно развивающееся, электронные обменные пункты с каждым днем становятся доступнее, а электронная наличность — ликвиднее.

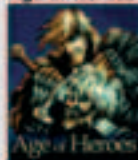
сверху вниз:
Способы оплаты в
WebMoney Transfer
Незатейливый
дизайн сайта E-gold



НЕ ИЩИ
МИНИМАЛЬНЫЙ
ПРОЦЕНТ — НЕ
РИСКУЙ, ИНАЧЕ
ОСТАНЕШЬСЯ
С НОСОМ

РЕКВИЗИТЫ
ПЕРЕХВАТЫВАЮТ
С ПОМОЩЬЮ ТРОЯ-
НОВ, КЕЙЛОГГЕ-
РОВ И СНИФЕРОВ

Age of Heroes: Армия Драка



Код загрузки: 36149
 Над миром вновь нависла угроза падшего драка, мертвые встали из своих могил, чтобы очистить землю от живых, им грозит вечный голод и чья-то злая воля.

Тебе предстоит спасти человечество от порождений тьмы. Путь героя нелегок, его поддерживает ослепительная магия и сложные задания, но опасные войны готовы происходить к твоей армии, а те, кто на светлой стороне, ищут правильный путь. Магия и артефакты надежно послужат тебе. Спаси мир от нечести!

Christmas Chix



Код загрузки: 36414
 Christmas Chix - это увлекательная аркадная игра, в которой Вам предстоит открывать скрытые изображения прекрасных девушек в самых сексуальных рождественских нарядах. Вам нужно будет заполнять игровое поле и в то же время избегать различных артов. Christmas Chix содержит 40 уровней, сложность их увеличивается по мере прохождения игры. В уровни содержится 9 разных картинок с рождественскими девушками. Дружественно, наслаждайтесь самой эротичной рождественской игрой для мобильных телефонов! И не полагайтесь!

Pizza Magnite



Код загрузки: 36415
 Стань на время владельцем пиццерии и защищи свою динет! Пусть конкуренты в ужасе закрывают свои заведения и подписывают документы о банкротстве. Теперь твои враги стали настоящим магнитом на рынке пиццы!

Стать известным не просто, ведь есть опасные конкуренты и бандиты, неблагоприятные районы и неуверенные посетители, отпугивающие покупателей. Необходимо принимать правильные решения, чтобы не допустить провала.

Real Tournament



Код загрузки: 36416
 Это настоящий командный экшн для мобильного телефона. Не важно, какая игра вам больше по душе! Дзюдо или Зенит флаги, - в любой игре вы сможете использовать лафты, поводы и конические подопалы с ножами-бастирами. Качественный искусственный интеллект составит вам достойную конкуренцию, а продуманные уровни заставят вас выбирать подходящую тактику в зависимости от ситуации. Убивайте соперников, копируйте с ними оружие. И пусть преподу "беты" - покажите, кто главный на арене!

Russian Star - Krystina



Код загрузки: 36189
 Russian Stars. Волнующая и обаятельная супермодель Кристина из России. Вы будете потрясены ее красотой, Вы не сможете провосторить ее страсти. Вы будете очарованы ее соблазнительной фигурой. Сегодня она будет позировать специально для Вас.

Russian Stars - это великолепное качество снимков, волшебное шоу соблазнов с беспрецедентно удобным управлением и великолепными возможностями. Соблазнительная и волнующая русская супермодель Кристина силой своей страсти очарует Вас.

Shark Fishmageddon



Код загрузки: 36413
 Жизнь водного мира, такая она есть - ешь быстро, или умри голодом! Ты маленькая акула, у которой есть шанс стать большой и неуязвимой. Журай разнообразных рыбок и раздробляй бонусы, закусывая вкусными аватарками, уберечь от вооруженных до зубов ловцов акул, которые, кстати, тоже годятся в пищу. Главное, помни - есть надо быстро и спастись так акул, что больше тебя по размеру. Впервые в одной игре тебе доступны те две разные версии: "Shark Fishmageddon" и "Shark Evolution".

Sirlitz



Код загрузки: 36150
 Самая веселая бродилка для мобильных телефонов позволит Вам погрузиться в борьбу с коварным диктатором. Откажитесь от обычной и его солдат. Лопайте различные предметы, все тайны и секретные бункеры.

Случай не придется, ведь предстоит пройти 15 уровней в 3 совершенно разных мирах, противоянием более 300 уровней. Горы разнообразных противников, мощное оружие для их уничтожения и отличная физика игрового движка - вот чем отличается "Sirlitz" от других подобных игр.

Бумер



Код загрузки: 36147
 ...По ночным улицам Москвы мчится черный BMW, уходящий от полиции. Цепь роковых событий с разборами и стрельбой поставила четырех героев - четырех друзей - вне закона. И в жизни без правил им нет пути назад...

Тебе предстоит уходить от полиции, сопровождать дальних друзей, встречать в разборы и стрелять. Даже на дороге, которую лучше не выбирать, приходится постоянно доказывать, что лучше тебя нет никого. А как это сделать - всепокая фильм, он будет самой лучшей подражкой.

Инструкция по запуску:

- 1) Создайте SMS-сообщение, в котором укажите код загрузки игры;
 - 2) Отправьте созданное SMS-сообщение на короткий номер 9955*;
 - 3) Дождитесь прихода ответного SMS-сообщения, содержащего ссылку на игру;
 - 4) Используя WAP браузер Вашего телефона, перейдите по полученной ссылке и осуществите загрузку и установку выбранной Вами игры.
- Стоимость игры: \$2.5/75 руб. (без НДС)**

9955

* для абонентов «Мобиль» короткий номер 9955

Получи убойный анекдот!

В самолете стюардесса спрашивает:
 - Нет ли в самолете врача?...
 Хотите узнать окончание? Отправь А 9573 на номер 9988*

9988

* для абонентов «Мобиль» короткий номер 9988

Отправь А на номер 9988* и читай самые убойные анекдоты на любые темы: про женщин, о семье, о политике, автомобильные и другие. Хотите получать анекдоты бесплатно? Отправь А AD на номер 9988*! Если отправил А TH на номер 9988*, получишь анекдот на рубрик «Народный анекдот!»

Стоимость \$2.5/75 руб. (без НДС)

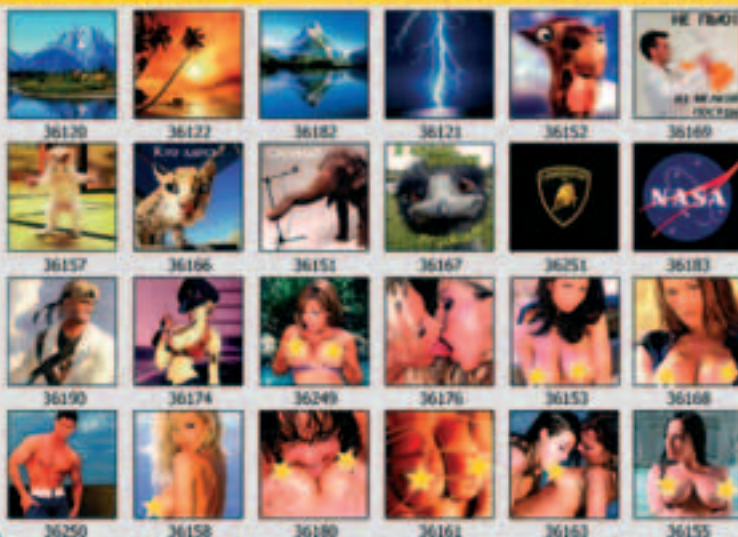
Запретных тем НЕТ!

9988

9988

* для абонентов «Мобиль» короткий номер 9988

Цветные картинки



Новый Тог!



Отправь SMS на короткий номер*

Мелодии

Стоимость сообщения \$0,75

Исполнитель / Название	Полифония	Нокиа	Майкрософт (Symbian)	Самсунг (J2ME)
ABBA / Happy New Year	36422	3642201	3642203	3642202
Axel F / Crazy Frog	36123	3612301	3612303	3612302
Crazy Frog / Popcorn	36197	3619701	3619703	3619702
David Guetta / The World is Mine	36115	3611501	3611503	3611502
Depeche Mode / Precious	36200	3620001	3620003	3620002
George Michael / Last Christmas	36424	3642401	3642403	3642402
Jingle Bells	36423	3642301	3642303	3642302
Moby / Lift Me Up	36133	3613301	3613303	3613302
Katrina / No Fear	36196	3619601	3619603	3619602
Robbie Williams / Tropic	36195	3619501	3619503	3619502
Timo Naas / Billionaire / First Day	36125	3612501	3612503	3612502
Братья Гримм / Кустурка	36193	3619301	3619303	3619302
В лесу родился елочка	36421	3642101	3642103	3642102
Венерия и Федорoff / Кавказская пленница	36135	3613501	3613503	3613502
Дельфин / Серебро	36199	3619901	3619903	3619902
Дискотека Авария / Новогодняя	36417	3641701	3641703	3641702
Корни / 25 Этаж	36126	3612601	3612603	3612602
Куриньемы / Запад (9 раз)	36192	3619201	3619203	3619202
Taty / All About Us	36191	3619101	3619103	3619102
МФ Ну погоди / Песня Зайки и Волка	36420	3642001	3642003	3642002

Звуки

Женский крик	36142	Смех	36408
Джингелский смех	36407	Гром	36143
Идейские барбаны	36137	Голос робота	36146
Звонок старого телефона	36138	Родственная игра	36139
Водяная трещка	36410	Говорящая утка	36409

Инструкция

Для получения мелодии или картинки просто SMS-сообщением, содержащим код на короткий номер 9922 (* для абонентов «Мобиль» короткий номер - 6622). Вам придет сообщение, содержащее мелодию или картинку (либо ссылку). Ссылка действительна в течение 24 часов. В случае свободного доступа, услуга будет считаться бесплатной. Для получения полифонических мелодий, а также для загрузки картинок необходимо подключить услугу WAP-ПРИЕМ и иметь операторов.

Полифонические мелодии доступны для мобильных телефонов: Nokia и Samsung.
Монофонические мелодии доступны для одноязычных телефонов: Alcatel, Motorola, Lexitel, Pantech, Philips, Siemens, Sanyo, Sharp.
SMS-мелодии доступны для одноязычных телефонов: Alcatel, Motorola, Lexitel, Pantech, Philips, Siemens, Sanyo, Sharp.
СТОИМОСТЬ загрузки и отправки байбайнов: Еврокомм - 0,5 (без НДС), HTC - 0,5 (без НДС), «Мобиль», «Мегасон», Телел, Релик, Цифровая Экспресс, МТК - 0,75 (без НДС) (для игр - 1,25); Нордволд GSM, Ульманс GSM, ОН (Патент-Т), Лидер (Ком. Архивенко, Екатеринбург) - 35 руб. (без НДС); ОН-GSM (Самара), Астрахань-GSM, «Мобиль» - 23 руб. (без НДС); УралкавказФон - 25 руб. (без НДС) (для игр - 75 руб.); Восточные SMS - бесплатно.

Служба поддержки mobile.support@relax.ru.
 ООО «Релакс» - крупнейший разработчик игр и приложений для мобильных устройств. «Восточные Экспресс», «Нордволд GSM», «Ульманс GSM», «Мобиль», «Мегасон», «Телел», «Релик», «Цифровая Экспресс», «МТК», «Астрахань GSM», «Астрахань GSM», «УралкавказФон», «Ульманс GSM», «ОН (Патент-Т)», «Лидер (Ком. Архивенко, Екатеринбург)», «МТК», «Астрахань GSM», «Астрахань GSM», «Мобиль» - 23 руб. (без НДС).
Торговые марки являются собственностью их владельцев.
 Лицензия №33353 выдана Федеральной службой по надзору в сфере связи



автоматический обменник

ROBOXCHANGE.COM

ROBOXCHANGE.COM — ОДИН ИЗ ПЕРВЫХ В МИРЕ И ПЕРВЫЙ В РУНЕТЕ АВТОМАТИЧЕСКИЙ ОБМЕННИК, КОНТРОЛИРУЮЩИЙ НА ДАННЫЙ МОМЕНТ БОЛЕЕ 50% ЭТОГО РЫНКА. ПРЕДСТАВИТЕЛЮ ROBOX МЫ ЗАДАЛИ НЕСКОЛЬКО ВОПРОСОВ ПО ТЕМЕ | **АНДРЕЙ КАРОЛИК**

По сути, деятельность обменного центра **robexchange.com** сводится к трем основным направлениям: непосредственно мгновенный обмен, предоставление интернет-магазинам услуг эквайринга электронных валют (таковой является мультивалютная касса **robexchange.net**), а также организация выпуска и процессинга скретч-карт для мгновенной оплаты интернет-проектов. Здесь принимаются к оплате практически все виды электронной валюты, платежи в которых мгновенны и безотзывны. В том числе, **robexchange.com** впервые на рынке начали осуществлять мгновенные переводы электронной валюты на банкоматную карту. К тому же ус-

лугами **robexchange.com** по приему оплаты пользуются практически все лидирующие онлайн-игры.

XS: В ЧЕМ СУТЬ ОБМЕННЫХ ЦЕНТРОВ? И ПОЧЕМУ ЭТИ ФУНКЦИИ НЕ БЕРУТ НА СЕБЯ САМИ ПЛАТЕЖНЫЕ СИСТЕМЫ?

СЕРГЕЙ ПОЛЯНСКИЙ: Суть понятна из названия: обмен одних электронных денег на другие. Платежные системы являются конкурентами, поэтому они не могут и не хотят брать на себя эти функции.

XS: НАСКОЛЬКО ЛЕГКО СОЗДАТЬ СОБСТВЕННЫЙ ОБМЕННЫЙ ЦЕНТР С НУЛЯ?

СЕРГЕЙ ПОЛЯНСКИЙ: На первый взгляд кажется, что легко. В roboxchange.com мы ежедневно получаем письма примерно следующего содержания: «Не могли бы вы продать скрипт вашего обменного пункта». Больше всего веселит в этом слово «скрипт». Видимо, со стороны это видится именно так. А на самом деле в создание надежного программного обеспечения для нашего проекта вложен не один десяток человеко-лет/трудозатрат. И именно поэтому мы являемся сегодня лидером этого рынка.

XS: ЕСЛИ ЛИЦО ПЛАНИРУЕТ СТАТЬ ПОСРЕДНИКОМ МЕЖДУ ПЛАТЕЖНЫМИ СИСТЕМАМИ, ТРЕБУЕТСЯ ЛИ ЗАКЛЮЧЕНИЕ ДОГОВОРЕННОСТЕЙ МЕЖДУ СТОРОНАМИ? НИКТО НЕ МЕШАЕТ ИСПОЛЬЗОВАТЬ СОБСТВЕННЫЕ КОШЕЛЬКИ...

СЕРГЕЙ ПОЛЯНСКИЙ: Безусловно, нужны. Со всеми платежными системами, с которыми работаем, мы связаны партнерскими договорами.

XS: ПОТРЕБНОСТЬ В ОБМЕНЕ ЗНАЧИТЕЛЬНО ВЫШЕ, ЧЕМ МОГУТ ОБЕСПЕЧИТЬ СУЩЕСТВУЮЩИЕ ОБМЕННЫЕ ЦЕНТРЫ. ПОЧЕМУ ЖЕ ИХ ТАК МАЛО?

СЕРГЕЙ ПОЛЯНСКИЙ: Обменные центры появляются и исчезают просто потому, что "скрипт" не обеспечивает стабильной и безопасной работы. Как правило, после полугода работы таких замороженных «менял» пропавшие из их обменника деньги тщетно разыскивают по всему интернету, а клиенты остаются «с носом». Именно поэтому обменник обменнику рознь. К сожалению, многие пользователи этих услуг смотрят только на комиссии, обращая мало внимания на такой фактор, как надежность. А потребности в обмене в состоянии обеспечить один roboxchange.com. У нас достаточно для этого и технических, и финансовых возможностей.

XS: КАКИЕ ОБМЕННЫЕ ОПЕРАЦИИ ДОМИНИРУЮТ В ДЕЯТЕЛЬНОСТИ ROBOXCHANGE.COM?

СЕРГЕЙ ПОЛЯНСКИЙ: Конечно, операции с лидирующими валютами на рынке. Это, безусловно, WebMoney и «Яндекс.Деньги». Впрочем, roboxchange.com активно развивается еще и как эквайрер электронных валют в пользу разных поставщиков услуг и товаров в интернет. Такие операции тоже занимают существенное место в roboxchange.com.

XS: КАКИЕ СУЩЕСТВУЮТ ГАРАНТИИ ПРИ ИСПОЛЬЗОВАНИИ ОБМЕННОГО ЦЕНТРА НА ТО, ЧТО СОБСТВЕННЫЕ СРЕДСТВА НЕ ПРОПАДУТ БЕССЛЕДНО?

СЕРГЕЙ ПОЛЯНСКИЙ: Гарантией является, прежде всего, репутация центра, его известность, признание основными платежными системами.

XS: РАСПРОСТРАНЯЮТСЯ ЛИ КАКИЕ-НИБУДЬ ЗАКОНЫ НА ДЕЯТЕЛЬНОСТЬ ОБМЕННЫХ ЦЕНТРОВ ИЛИ ВСЕ ДЕЛАЕТСЯ ВНЕ ЗАКОНА?

СЕРГЕЙ ПОЛЯНСКИЙ: Да, конечно. По сути, платежные системы являются платежными агентами для обменного центра, а он сам является таким же агентом по отношению к поставщикам цифровых товаров и услуг. Отношения с пользователями регламентируются договором мены.

XS: КАК СЛЕДУЕТ ВЫБИРАТЬ ОНЛАЙНОВЫЕ ОБМЕННИКИ, ЧТОБЫ НЕ ПРОКОЛОТЬСЯ?

СЕРГЕЙ ПОЛЯНСКИЙ: Все как в жизни, ничего нового. Надо выбирать надежные, давно существующие, проверенные, такие как roboxchange.com :).

XS: СЛУЧАЮТСЯ ЛИ АТАКИ НА ОБМЕННЫЕ ЦЕНТРЫ? КАКОГО РОДА?

СЕРГЕЙ ПОЛЯНСКИЙ: Да, постоянно. Чаще всего DDoS-атаки.

XS: КАКОВА ВАША ПОЛИТИКА БЕЗОПАСНОСТИ?

СЕРГЕЙ ПОЛЯНСКИЙ: Мы работаем в тесном контакте со всеми платежными системами и правоохранительными органами многих стран, где в ходу находятся электронные деньги, с которыми работает roboxchange.com, — от родной милиции до ФБР и Скотленд-Ярда.

продайся за e-money!

ИЛИ КАК СТАТЬ ВИРТУАЛЬНОЙ РАБЫНЕЙ

ХОЧЕШЬ УЗНАТЬ РЕАЛЬНЫЙ РЕЦЕПТ ТОГО, КАК ЗАРАБОТАТЬ КУЧУ ДЕНЕГ, НЕ ВСТУПАЯ В КОНФЛИКТ С ЗАКОНОМ — ТОЛЬКО СО СВОЕЙ СОВЕСТЬЮ? НЕ ТРЕБУЕТСЯ НИКАКИХ НАЧАЛЬНЫХ ВЛОЖЕНИЙ, ТОЛЬКО КОМПЬЮТЕР, ИНТЕРНЕТ (НЕ ОБЯЗАТЕЛЬНО СКОРОСТНОЙ) И ЗНАНИЕ АНГЛИЙСКОГО ХОТЯ БЫ НА УРОВНЕ СРЕДНЕЙ ШКОЛЫ. ЭТО НЕ МОШЕННИЧЕСТВО! ТОЧНЕЕ, МОШЕННИЧЕСТВО, НО НЕ В УЩЕРБ ТЕБЕ | **ЛОСЬ АКА СЕВЕРНЫЙ ОЛЕНЬ**





Кто из нас не мечтает разбогатеть? К примеру, автор статьи об этом точно не мечтает: у него скромные потребности, он не обращает внимания ни на мир, ни на тело, в котором живет. Для счастья ему вполне достаточно отладчика, дизассемблера и компилятора :). Если бы на него свалился мешок денег, он бы не придумал, на что тратить. Впрочем, все это лирика. Большинство нормальных людей имеют совсем другое мнение на этот счет (например «денег много не бывает»), только не все умеют зарабатывать их. В интернете постоянно образуется множество пирамид, но на них уже никто не ведется, так что даже сам создатель пирамиды практически ничего не получает. Создать свою пирамиду и раскрутить ее с нуля сегодня практически нереально. Как минимум, требуется свежая идея. Наверняка твой e-mail регулярно забрасывают кучей электронной макулатуры, предлагающей различные способы заработка практически без вложений, но за каждым из них стоит какой-то подвох. А реально ли заработать не прибегая к мошенничеству?

Это вполне возможно. И один из способов мы подглядели, хотя никогда не применяли его на практике. Однако, как утверждают те, кто им занимается, схема работает. Мы отнюдь не первооткрыватели и совершенно случайно узнали о нем из разговоров с людьми, которые постоянно этим промышляют. Естественно, никаких деталей. Так... обрывки информации и тонкие намеки. Но мы все-таки реконструировали всю схему и воссоздали целостную картину, которая, как нам кажется, может сработать.

Ни в какой конфликт с законом мы не вступаем! Правда, существует ничтожная вероятность влететь в физические разборки с перспективой получения телесных повреждений, но шансы один из миллиона. Также имеются и некоторые другие проблемы, но в целом все достойно и нормально. Кто не хочет, дальше может не читать :). Мы ничего не навязываем и ни к чему не агитируем. Напротив, мы хотим показать, как в интернете кролики становятся жертвами, чтобы в один прекрасный день ты не побывал в шкуре «разведенного» кролика! Мы никогда не пытались проделать это, поэтому все рассуждения относятся к области теоретической абстракции.

Суть идеи Известно, что все американцы — инфантильные и слабомыслящие, особенно это справедливо по отношению к коренным. Англичане — еще более крутой атас. Русские тоже, кстати, не подарок. Например... грузины. Те в любом месте найдут, с кем переспать! Это не упрек, а, скорее, восхищение. Пока мы, русские, чешем свой инфантилизм в гордом одиночестве, наши девушки извиваются под... То есть это уже не девушки и не наши. Так что двойной облом. Познакомиться с девушкой (особенно имея серьезные намерения) не так-то просто даже у нас, не говоря уже о дальнем-дальнем зарубежье.

Вот цитата из замечательной истории «Как перестать программировать и начать жить» от Перси Шелли. Для начала усвой: все, что ты знал об американских женщинах, — миф. Твой мысленный десктоп полнят иконки стройных и доступных телок, а на самом деле такие девайсы грузятся только на скотобазах Голливуда. Но куда ужаснее другое. Ты привык к российским женщинам, которые сами бегают за мужиками. Причем эта привычка подсознательная: внешне все выглядит так, словно рулят мужики. И только очень опытный программист знает, что женщины в России и по численности, и по биологической активности обгоняют мужиков — слишком уж покоялись наших папочек войны, алкоголь и прочие эксперименты властей. В стране ковбоев все иначе. В обычном штатовском баре на полсотни мужиков едва наскребется одна девица, у которой вогнутая талия и выпуклая грудь, а не наоборот. С девицей обязательно компания из ее бойфренда и трех бывших бойфрендов. Все остальные сорок пять ковбоев видят себя Ее будущими бойфрендами и глаз с Нее не спускают. В такой аэродинамической трубе девишке остается только крутить своими выпуклыми частями. А потом, когда начнется драка, сигануть к двери и ждать того, чья голова не будет хакнута табуреткой :). Именно из-за такой несовместимости интерфейсов женатый русский програм-

РУССКИЕ
ДЕВУШКИ —
МЕЧТА МНОГИХ
ТОЛСТОСУМОВ

ЗАРАБОТАТЬ МОЖНО
И НЕ НАРУШАЯ
ЗАКОНОВ

мист в Америке быстро теряет свою жену (смотри выше). И еще из-за этого в Штатах ты легко можешь оказаться в тюрьме за действия, которые у русской женщины вызвали бы лишь хихиканье. Прошелся по улице вслед за американкой — она легко посадила тебя на пять лет. Ущипнул ее за одно место — тебе светит еще больше. Первое называется «секшувал харасмент», конкретнее «сталкинг». А второе — «секшувал ассолт», конкретнее «анал пене-трейшн». Запомни термины — пригодится в беседе с адвокатами :). Ты спрашиваешь, неужели они не хотят? В кино они занимаются сексом и в лифтах, и в бассейнах, и все такое. Проблема в том, что на самом деле «всем таким», включая наркоту и госк-n-roll'ы, у них занималось прошлое, родительское поколение. По гегелевско-тургеневскому принципу это привело к тотальному обессексиванию, опосению и вообще консерватизму нынешнего поколения. Ты, наверное, в курсе, что если американцы хотят позаниматься сексом, они приглашают друг друга на обед. Но ты не в курсе, что этот идиотский обычай (кто, скажи, занимается этим с набитым желудком?) соблюдается очень жестко. То есть если ты приглашаешь американскую женщину поесть вместе, у нее в системном блоке сразу загорается красная лампочка: «Караул, меня хотят трахнуть!» И полиция уже тут как тут. Пять лет минимум.

Конечно, это шутка. Если ты был в Америке или общался с тамошними туземцами, ты только посмеешься. Но суть такова! Посмотри на реальных американок. Ой, нет, лучше не надо. Они все толстые и какие-то не такие... не возбуждающие, зато с большим самомнением. А даже такую хрюшку найти ох как сложно. Женщин мало, мужиков много, да и тех засосала сплошная круговерть работа-дом-работа. Вроде бы все есть для счастья, а самого счастья-то нет. Девушку нужно. Ни для кого не секрет, что на девушек из России существует огромный спрос. Девушки из Азии идут тоже. Нет, речь не о проституции, речь о... банальном замужестве.

Отчаявшись найти девушку у себя, многие американцы (и другие народности) обращают свой взор к загранице. Любой американский бизнесмен с внешностью из серии «я столько не выпью» уверен на все 100%, что для наивной русской девушки он будет неотразимым ковбоем, даже если его един-

ДЛЯ РАЗВОДА НУЖНО НЕПЛОХО ЗНАТЬ ПСИХОЛОГИЮ ЧЕЛОВЕКА И ХОРОШО ЧИТАТЬ/ПИСАТЬ НА АНГЛИЙСКОМ

МНОГИЕ НЕУДАЧНИКИ ИЩУТ СВОЮ СУДЬБУ В СЕТИ

ственная лошадь — горбатый «Форд» цвета б/у. Короче, он лезет в интернет и...

Вот, собственно, и все. Остается только разместить свое объявление и пожинать урожай. Мужики идут косяками. Главное — правильно тянуть из них деньги так, чтобы они клевали, а ты только успевал подсекать.

ПСИХОЛОГИЯ ЖЕРТВЫ Извлечь выгоду из общения с мужиками просто так не получится. Они хоть и американцы, но совсем не дурные, и кое-какой опыт распознавания «разводов» у них тоже имеется. К тому же, конкуренция в этом секторе «рынка» просто огромна. Девушки (настоящие) становятся в очередь, вытесняя псевдо в самый хвост. Солидные сайты знакомств обычно проверяют данные, указываемые при регистрации, к тому же за размещение объявления требуют денег, расставаться с которыми в наши планы никак не входит.

Жизнь западных людей — это жизнь роботов и растений. Сверху давит правительство, снизу — начальство, и ходить можно только по струнке. Хочется встряхнуться, хочется уйти от сытой жизни в совершенно другой мир. Мир тайных желаний и нереализованных фантазий. Именно поэтому BDSM (садомазохизм) стал так популярен. Существует куча сайтов, на которых так называемые мастера вербуют рабов.

Мастера — это просто закомплексованные типы, их не любили девочки, в школе их дубасили сверстники, поэтому... Надо же как-то самоутвердиться в жизни! Настоящие (true) мастера никогда не заходят на BDSM-сайты в поисках рабов. Они имеют Силу, дарованную природой. Дар управлять людьми. Если мастер чего-то хочет, он просто идет на улицу, выдергивает первого попавшегося человека, который ему понравился и... Нет, гипноз тут ни при чем. Обычное знакомство, быстро перетекающее в дружеские отношения и т.д. Но мастер легко ломает любого (или не совсем любого) человека, заставляя делать все, что заблагорассудится его величеству. Как минимум, мастер должен владеть словом, то есть отдавать приказ так, чтобы человек выполнил его раньше, чем успел осознать. Ты не поверишь в это, пока сам не испытаешь на себе.

Вернемся к рабам. Как в анекдоте, встретились садист и мазохист. Мазохист говорит: «Ну, мучай же меня». А садист: «А вот и не буду». На самом деле рабы — это те же мастера, только недоразвитые или еще не открывшие себя. Во всем должен существовать баланс (equilibrium). Если человеку дарована сила, ему также даровано стремление подчиняться. Парадоксально, но факт. Рабы используют мастеров как игрушку для получения удовольствия, грубо говоря, как вибратор.

Большинство обитателей BDSM-сайтов и форумов знакомств — это вполне нормальные люди, только слегка больные :). Они живут в мире фантазии, которую в той или иной степени претворяют в реальность. Однако рабы довольно быстро посылают своих мастеров: ожидали увидеть действительно сильную личность, а не кусок чего-то неаппетитного без фантазии, без силы, без притягательности.

И тут на сцену выходим мы :). Даем объявление от девушки-рабыни, готовой абсолютно на все и в первую очередь на переезд в другую страну. Как говорится, устоять невозможно. Но вот тут-то и начинается самое интересное. Ответы мастеров, в грубом приближении, можно разбить на две категории или типа. Первый: с виду вполне нормальные люди, которым достаточно, чтобы рабынька работала по хозяйству на халяву, носила ошейник, возможно, была постоянно голой. Воск и фистинг прилагается. А вот второй тип: сразу без обид предлагают жизнь в клетке, пять кобелей будут насило-

Заполни форму и начни поиск жертвы, которая так стремится с тобой познакомиться :)



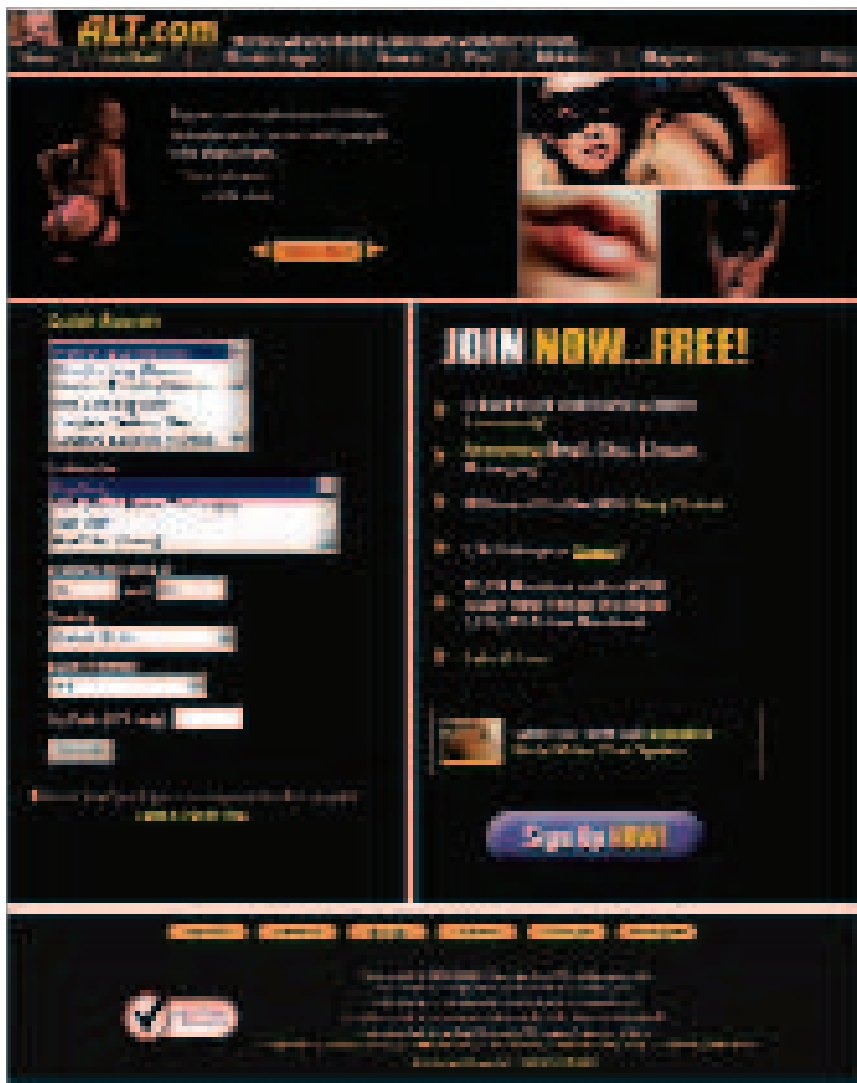
вать тебя связанную, дальше лучше не продолжать... Интересно, существует ли рабыня, которая действительно хочет всего этого? Уверен, что нет. На самом деле это просто игра: обмениваешься своими фантазиями и совсем не собираешься реализовывать их, но делаешь это как бы всерьез, как бы взаправду — Малый театр в чистом виде. Весь фокус в том, что, когда дело заходит достаточно далеко, мастер действительно высылает «рабыне» деньги (немалые) на «переезд», хотя и так знает, что она не переедет. Невероятно, но факт!

Что же до мастеров из первой категории, то... На долгую переписку с ними рассчитывать не стоит. Они сразу же требуют номер телефона, звонят тебе (или просят установить web-камеру), сами прилетают в Россию, чтобы забрать тебя :). Вообще-то можно развести и их, но смысл? Второй тип предпочтительнее. Во-первых, ты имеешь кучу «компромата»: письма, детально описывающие, что они «делали» (как и с кем), множество присланных ими по-настоящему садистских фотографий, надерганных с интернета. Кстати, определить реальный адрес такого мастера довольно просто. Даже если он сидит за прокси, он дает свой телефон или что-то вроде того. Во-вторых, переводя деньги тебе, такой мастер не слишком-то надеется на приезд рабыни, так что будет не очень огорчен. Но это все теория. Переходим к практике.

как действуют мошенники Самая сложная часть операции, от которой на 98% зависит количество вовлеченных мастеров, — поиск подходящей фотографии. Интернет буквально кишит всякими фотографиями. Как говорится, выбирай — не хочу, но «всякая» фотография не подойдет. Требуется найти девушку не красавицу, не уродину, с затравленным взглядом (хорошо подходящим для рабыни), при этом не полную дуру. В общем, такую, на которую повелся бы и сам :). Желательно, чтобы у тебя было несколько ее фотографий в разных позах и различных обстоятельствах (по месту и времени). Наличие интимных фото очень желательно, но найти что-либо в Сети по таким критериям практически нереально. Как искать? Очень просто: в Google по именам. Только имена должны быть не русскими, а... скажем, польскими. Что-то среднее между востоком и западом. На многих серверах обычно удается обнаружить целые альбомы любительских фотографий — копай, обязательно найдешь. Только обязательно переименовывай фото перед тем, как отдавать кому-то, иначе тем же Google тебя сразу засекут и вместо развода получится сплошная фигня.

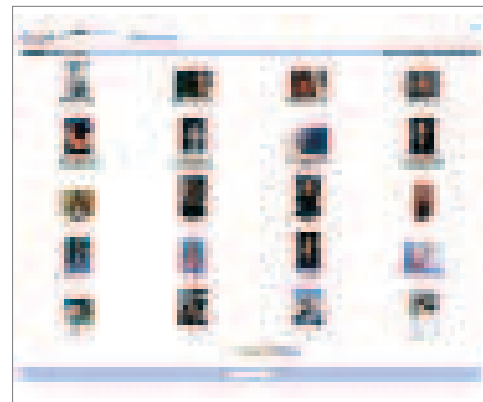
Затем необходимо найти подходящий сайт BDSM-знакомств. Крупнейший из всех, конечно, www.alt.com, но туда лучше не ходить — ты не справишься с таким табуном. Добыть деньги из мастера за неделю вполне реально, а если действовать на конвейере, то за это же время можно обработать и несколько десятков мастеров. Объем переписки на самом деле огромен, особенно если подходить к каждому письму творчески, а не пользоваться технологией cut-n-paste. Так вот, лучше размещать предложение услуг себя/девушки на заброшенном сайте со скромной и постоянно меняющейся аудиторией. Во-первых, там меньше объявлений от других «рабынь» (читай «мошенников»), а во-вторых, если даже кто-то и напишет «she is a faker», никто этого не заметит и через некоторое время ты сможешь снова зарегистрироваться под другим именем.

Как находить такие сайты? А Google на что? Ищи по комбинациям «looking for master», «seeking master», «[female] sub wanted» и т.д. Только предельно позаботься о хорошем прокси. Причина даже в не в том, что в случае провала к тебе могут прийти и начистить какую-либо часть тела (в чужой стране никакой мастер хозяйничать не станет) — многие модераторы отслеживают мошенников, а на «засвеченные» IP ставят бан, так что повторная регистрация становится невозможной.



МОЖНО НЕ СОЧИ-
НЯТЬ СВОЮ ЛЕГЕН-
ДУ С НУЛЯ, А ПОЗА-
ИМСТВОВАТЬ ЕЕ В
ИНТЕРНЕТЕ

сверху вниз:
Популярный BDSM
портал www.alt.ru
Результат поиска
фото на Google



ТЕКСТ ОБЪЯВЛЕНИЯ Писать о себе, красивой и безумной, нужно так, чтобы клюнули. Естественно, на английском. Не обязательно на хорошем, но, по крайней мере, на доступном для понимания. Что именно предлагать и в каких количествах... Тут возможно множество вариантов. С одной стороны, если ты просто предложишь стать женой/домохозяйкой, готовой к сексу в любое время, на это клюнет только первый тип мастеров, непродуктивность которого мы уже обсуждали. С другой стороны, если предложить сжечь себя на слабогорящем костре, то даже фантазеры лишь хихикнут и вряд ли ответят. А если и ответит, то только бедная молодежь))

Вот неплохой образец, выловленный в Сети. Неизвестно, кто эта девушка. Может, она действительно реальная мазохистка с больной головой :), но почему-то мне кажется, что это классический мошенник.

1 Female sub offers her body-n-soul to real 24/7 master

I'm young 20 years old slut. I'm skin and pretty beautiful.
I'm a masochistic slave by nature. I like pain.

I want to be punished, abused, humiliated, spanked and ****d.
I haven't any limits and stop words.

This means that you may do everything what you want to do.
I'm ready to real torture and pain. I don't expect pleasure in any way.
You may deform my body in your own way. I don't afraid hurts.

I want to be your toy and sexual servant without any right.
I can be housemaid and I'm good housemaid.
I want live in your house (even outside),
I don't pretend on private room,
I'm ready to be totally nude and exposed.

I think, I live very long from you, but I'm ready to relocate at any place.
I wish to find extreme sadist — man or women.
But, if you just want to have a good maid or whore for free let me by.

перевод: «Женщина-рабыня предлагает свое тело и душу реальному мастеру на 24 часа и 7 дней в неделю. Юная 20-летняя потаскуха. Худенькая, да и лицом тоже ничего. Мазохистка по натуре. Люблю боль. Хочу быть наказанной, третируемой, униженной, отшлепанной и изнасилованной. У меня нет лимитов, и я не знаю слов «стоп, уйди, поганый». Ты можешь делать со мной все, что хочешь. Готова к реальным пыткам и боли. Никакого удовольствия я не ожидаю. Ты можешь уродовать мое тело по своему собственному усмотрению. Повреждений не боюсь. Хочу быть твоей игрушкой и секс-служгой без каких бы то ни было прав. Могу быть хорошей домохозяйкой. Хочу жить в твоём доме (даже снаружи), на отдельную комнату не претендую, готова быть полностью обнаженной и выставленной напоказ. Думаю, что живу далеко от тебя, но готова к переезду в любое место. Желаю найти экстремального садиста, мужчину или женщину. Если ты хочешь завести хорошую хозяйку или проститутку на халаву — дай мне знать».

Обрати внимание на то, что место жительства никак не указывается. Действительно, зачем сразу афишировать, откуда ты? Об этом ты скажешь потом. Правда, спектр предоставляемых услуг несколько сбивает с толку. Молодая 20-летняя девушка и вдруг хочет чего-то очень непотребного :). И ведь нет чтобы пойти к ближайшему бомжу — она ломится далеко за границу. Зачем?! Но у рабыни на все готов ответ. Читаем следующий пост.

2 Sorry, I did'n read this topic just received pm
as far as meseems I've found my Master!
He don't take me yet. we're just emaling.
I hope he'll own me, but I'm not 100% sure that He a top at all.
I saw many tops, not true master but top.
I know how to recognize top, but I never can be sured
you now, this is common net problem.
nobody can be sured that other part not are liar or cyber.
ok. never mind. lets suggest that I'm taken

I'm really wish to pain and torture
this is the only way to redeem my sins.
this is a long story...
back in the old days I playing with peoples.
I went around and broke hearts. I believed to nothing.

many good guy felt in love, but I didn't reciprocate.
six boys **** himself. at that time this didn't touch me. I just giggled.

but right now I REALLY scared by hellfire.
I'm a hard sinner and I know I can clear and save my soul only via violent
torture and pain. May be via burning on the slow fire or kind of.
I don't look for pleasure of being slave like many other slave probably do.
I just want to redeem my sins. after this the death will be my award and freedom
this is the reason why I look for Master far-far-far form my location.
local masters afraid **** me 'cause they keep authorities in mind

перевод: «Извини, не читала, только получала приватную почту. Как мне кажется, я нашла своего мастера! Он еще не призвал меня к себе. Мы просто занимается совместным онанизмом, прости, обмениваемся мылом. Я надеюсь, что он возьмет меня, но я на 100% не уверена, что он вообще топ. Я видела много топов, не настоящих мастеров, но все-таки топов. Я знаю, как распознать топа, но я никогда не могу быть уверенной. Знаешь, это типичная сетевая проблема. Никто не может быть уверен, что противоположная сторона не приколист и не виртуал. Ладно, неважно. Давай считать, что я уже взята. Я действительно хочу боли и пыток, это единственный путь для искупления моих грехов. Это длинная история, устраивайся поудобнее, расстегивай ремни, сейчас взлетать будем. Давным-давно я игралась с людьми. Я тусовалась с парнями и разбивала сердца. Я ни во что не верила. Много хороших парней влюблялись в меня, но я им не давала, в смысле, не отвечала взаимностью. Шесть парней убили себя. Тогда это меня совсем не трогало. Я просто ржала. Но сейчас... Я ДЕЙСТВИТЕЛЬНО боюсь адского пламени. Я жуткая грешница и знаю, что могу очистить и спасти душу только через дикие пытки и боль. Быть может, через сожжение на медленном огне или что-то типа того. Я не ищу удовольствия от бытия рабыней, как многие другие рабыни, возможно, ищут. Я просто хочу искупить свои грехи. После этого смерть будет наградой и освобождением. Это и есть та причина, по которой я ищу мастеров очень-очень-очень далеко от моего места жительства. Местные мастера боются убивать меня из-за страха перед властями».

Это же какую фантазию надо иметь, чтобы сочинить такую детективную историю! Правда, насчет шести парней она все-таки перегнула. Почему тогда не целый оркестр армии и флота в полном составе? Вполне хватило бы и одного самоубийцы, от силы двух. Зато появилась идея о сожжении на костре. Бред, конечно, но именно этим и заманивают. Обрати внимание, ни о каких деньгах речь пока не идет!

Также необходимо предусмотреть обходной путь. Мало ли что... Вдруг попадет психически неуравновешенный мастер, который станет угрожать (а таких большинство). Девять из десяти, что это просто подросток, и на него можно не обращать внимания. А чтобы не сильно досаждал, пишешь вот что.

3 I'm a journalist. I'm tracking down lost peoples. many girls had disappeared
at the last time. may be they was kidnapped and killed by maniacs.
I'm walking over net, offering myself as victim, determine the real name and
location my so-called «masters», and give it up to the authorities.

перевод: «Я журналистка. Занимаюсь поиском пропавших людей. Много девушек исчезло в последнее время. Возможно, они были похищены маньяками и убиты. Я блуждаю по Сети, предлагая себя в качестве жертвы, определяю реальные имена и местоположение так называемых мастеров и передаю эту информацию властям».

После этого, как показывает практика, пыл воинствующих мастеров сразу стихает и они исчезают в неизвестном направлении. Даже если они и не маньяки (что, скорее всего, так и есть), это же какие проблемы их ждут! Как минимум, родители узнают, что их любимое чадо ходит по всяким там порносайтам, да еще нестандартной тематики. Или об этом узнает босс. Вот будет радость! А что? История с журналисткой вполне убедительна.

когда финансы поют романсы Где же все-таки обещанные 100 000? Переписки — море, из-под пальцев буквально дым идет, а еще нужно напрягать фантазию, вызывать у мастера возбуждение, излагая свои мысли на чужеродном английском языке.

Несомненно, мастер спросит, готова ли рабыня перевести к нему за свой собственный счет (потому что платить ей он все равно не собирается) и как скоро. Отвечаешь что-то вроде: «I've some money, I think that it'll be enough. I haven't VISA yet, but I've started to make it, but it'll takes some time, I don't know how much exactly, I never left Russia before (У меня есть кое-какие деньги и я думаю, что их хватит. Визы нет, но уже начала ее получать. Это займет некоторое время, сколько именно — не знаю. Я еще никогда не выезжала из России)». И все ОК. Переписка продолжается, рабыня создает то впечатление, которое запланировала создать, но все никак не едет, каждый раз находя различные предлоги. В общем, мнется, а потом говорит, что, по правде говоря, деньги у нее, конечно, есть, но недостаточно. Дальше объяснять?

О переводах. Тут-то мы и подошли к электронным платежам вплотную. Как вариант, можно воспользоваться Western Union. Небольшие суммы (в районе до \$500) могут выдаваться без предъявления документов, удостоверяющих личность, достаточно описания некоторых внешних примет. Правда, у жертвы может возникнуть подозрение насчет того, почему рабыня боится показать свой паспорт. Именно поэтому некоторые изначально придумывают другую невероятную историю или сразу позиционируют себя как рабыню-нелегалку без документов, с большими проблемами с законом, но готовую ухать хоть к черту на рога, безвылазно жить в любом особняке, хоть голышом в клетке, только чтобы в тепле и кормили. Мастера ведутся со свистом навозной пули!

Естественно, предпочтительно использовать не прямой перевод WebMoney-WebMoney, к тому же эта система не распространена за границей. Лучше перебрасывать деньги через несколько платежных систем, чтобы запутать следы...

проблемы взаимопонимания Парни, учите английский. Английский — это вещь! Это великолепный инструмент для общения с жителями других стран. Английским владеют большинство цивилизованных людей. Испания, Франция, Швейцария... Даже Китай! Вместо того чтобы пользоваться по-своему несчастными мастерами, переписывайся с друзьями-программистами или фэнами любимых групп. Последние вполне могут пригласить тебя на концерт, предложив взять на себя все расходы. Всякий состоятельный (но не богатый) человек в определенный момент начинает ощущать жгучую потребность в самоутверждении. Пригласить человека из заснеженной России к себе в гости и взять все затраты на себя — отличный способ кинуть кучу денег на ветер со словами «Я многого добился в жизни, у меня есть деньги, и мне ничего не стоит исполнить мою любую прихоть». Попадаются, конечно, и жмоты (их большинство), но тебе же много и не нужно! Главное — выучить английский, а там...

Курсы «американского английского» а-ля Илона Давыдова отбросим сразу. Выучить язык можно только заставив себя. Достаточно выработать устойчивые языковые ассоциации, и тогда ты сможешь говорить и писать, возможно, даже сам не понимая, что говоришь, но это и не важно :). Главное — чтобы тебя понимали. К примеру, смотри американские фильмы в оригинале (сначала с субтитрами, потом без), читай книги, заведи себе друзей по всему миру. Но зубрить английский не надо — на нем нужно говорить.

напоследок Только не воспринимай все сказанное всерьез. И тем более не пытайся применять данный способ заработка на практике. Да, никакую статью тебе не пришлют: несмотря на то, что это явное мошенничество, состав преступления отсутствует. Ну... практически отсутствует. Это обычная афера. Лишь географическая, политическая и юридическая разобщенность мешает наказывать мошенников. Через некоторое время, быть может, через год или два, лавочка прикроется. Как говорится, МММ можно построить только однажды.

Лучше жить с чистой совестью и никогда не совершать правонарушений :). Зато за время переписки ты в совершенстве овладеешь английским — золотым дном. Знаешь, сколько сейчас стоят переводы?

ЧТОБЫ ЗАПУТАТЬ СЛЕДЫ, ОБЫЧНО ПРОВОДЯТ ПЕРЕБРОСКУ ДЕНЕГ ЧЕРЕЗ НЕСКОЛЬКО ПЛАТЕЖНЫХ СИСТЕМ.

НЕВЕРОЯТНО, НО ДЕНЬГИ МОГУТ ВЫСЛАТЬ ДАЖЕ ТОГДА, КОГДА ОЧЕВИДНО, ЧТО ОНИ УЙДУТ В НИКУДА.

Английский, как и любовь, воистину объединяет мир, не правда ли :)?



ГИД ПО КОШЕЛЬКАМ

КРАТКАЯ ИНСТРУКЦИЯ ПО ИСПОЛЬЗОВАНИЮ ПЛАТЕЖНЫХ ИНТЕРНЕТ-СИСТЕМ

ЧТО ТАКОЕ ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ И ДЛЯ ЧЕГО ОНИ ИСПОЛЬЗУЮТСЯ, МЫ УЖЕ ЗНАЕМ. ОСТАЛОСЬ РАЗОБРАТЬСЯ, КАК ИСПОЛЬЗОВАТЬ ИХ. К СОЖАЛЕНИЮ, ОБЪЕМ ЖУРНАЛА НЕ ПОЗВОЛЯЕТ РАССМОТРЕТЬ ВСЕ ПЛАТЕЖНЫЕ СИСТЕМЫ, ПОЭТОМУ МЫ ОГРАНИЧИМСЯ САМОЙ ПОПУЛЯРНОЙ НА ПРОСТОРАХ СНГ СИСТЕМОЙ — WEBMONEY. НА ЗАПАДЕ САМЫМИ ПОПУЛЯРНЫМИ ПЛАТЕЖНЫМИ СИСТЕМАМИ ЯВЛЯЮТСЯ PAYPAL И E-GOLD, ПОЭТОМУ ЕСЛИ ТЫ РАБОТАЕШЬ С ДАЛЬНИМ ЗАРУБЕЖЕМ, ОСВАИВАЙ ИХ САМОСТОЯТЕЛЬНО. НУЖНО ТОЛЬКО ОТМЕТИТЬ, ЧТО ЕСЛИ НА ЗАПАДЕ ЗА «ЭЛЕКТРОННЫЕ ДЕНЬГИ» МОЖНО КУПИТЬ ЧТО УГОДНО, ТО У НАС ВЫБОР ОГРАНИЧЕН, НО ЭТО ТОЛЬКО ВОПРОС ВРЕМЕНИ | ДЕНИС КОЛИСНИЧЕНКО

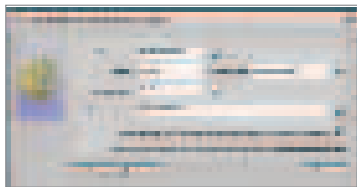
webmoney Это не какая-нибудь «виртуальная» контора, а самая обычная официально зарегистрированная компания. Главный офис расположен в Москве по адресу Каширское шоссе, дом 58, строение 3, тел. (095) 727-43-33. Подробности о работе системы можно прочитать на официальном сайте www.webmoney.ru. Если хочешь узнать больше, рекомендую неофициальный сайт — www.owebmoney.ru.

Думаю, не стоит подробно описывать возможности WebMoney. Это обычная платежная система, и ее функции не особо отличаются от функций других систем. С WebMoney ты можешь:

- ПОЛУЧАТЬ ДЕНЬГИ И ОПЛАЧИВАТЬ УСЛУГИ НЕ ВЫХОДЯ ИЗ ДОМА, ДАЖЕ НЕ ВСТАВАЯ ИЗ-ЗА КОМПЬЮТЕРА.
- РАССТОЯНИЕ, КОТОРОЕ РАЗДЕЛЯЕТ ОТПРАВИТЕЛЯ И ПОЛУЧАТЕЛЯ ПЕРЕВОДА, НЕ ИМЕЕТ ЗНАЧЕНИЯ: ЗА СЧИТАННЫЕ СЕКУНДЫ ТЫ ПОЛУЧИШЬ СВОИ ДЕНЬГИ ИЛИ ЖЕ ОТПРАВИШЬ ИХ НА СЧЕТ ПОЛУЧАТЕЛЯ.

Информация о пользователе

Зарегистрировать кошелек в системе WebMoney может кто угодно, даже необязательно гражданин России. Все, что нужно, — это компьютер, подключенный к интернету, и программа WebMoney Keeper, которая существует в двух версиях:



- КЛАССИЧЕСКАЯ (CLASSIC) — РЕАЛИЗОВАНА В ВИДЕ ОБЫЧНОЙ WINDOWS-ПРОГРАММЫ.
- ОБЛЕГЧЕННАЯ (LIGHT) — WEB-ИНТЕРФЕЙС, РЕАЛИЗУЮЩИЙ ФУНКЦИИ РАБОТЫ С КОШЕЛЬКОМ.

Первая версия подходит для домашнего использования, она устанавливается на твоем компьютере. Запускаешь ее как обычную Windows-программу и управляешь своим кошельком.

Вторая версия подходит для «мобильных» пользователей: если ты часто путешествуешь, то с помощью web-интерфейса WM Keeper Light сможешь управлять своим кошельком из любой точки земного шара.

Правда, есть варианты. Если у тебя ноутбук, на котором установлена Windows, то ты смело можешь устанавливать классику, только не забудь захватить в дорогу ноутбук. Если у тебя Linux, то даже на стационарном домашнем компьютере ты будешь вынужден использовать только WM Light, поскольку Linux-версии WM Keeper в природе не существует.

ставим Webmoney Keeper Classic В этой статье мы рассмотрим только классическую версию WM Keeper, потому что журнал не резиновый и на всех места не хватит.

Итак, заходи на www.webmoney.ru и качай полную версию WM Keeper — http://download.webmoney.ru/wm2_full.EXE, всего 2,5 Мб. Модем «средней паршивости» способен закачать ее примерно за 6-8 минут. Если же у тебя с интернетом вообще плохо, можно скачать урезанную версию WM Keeper — <http://download.webmoney.ru/wm2.EXE> (на ее загрузку уйдет 4-6 минут). Я рекомендую качать полную версию — все равно бесплатно. Кстати, для комфортной работы с WebMoney не помешает

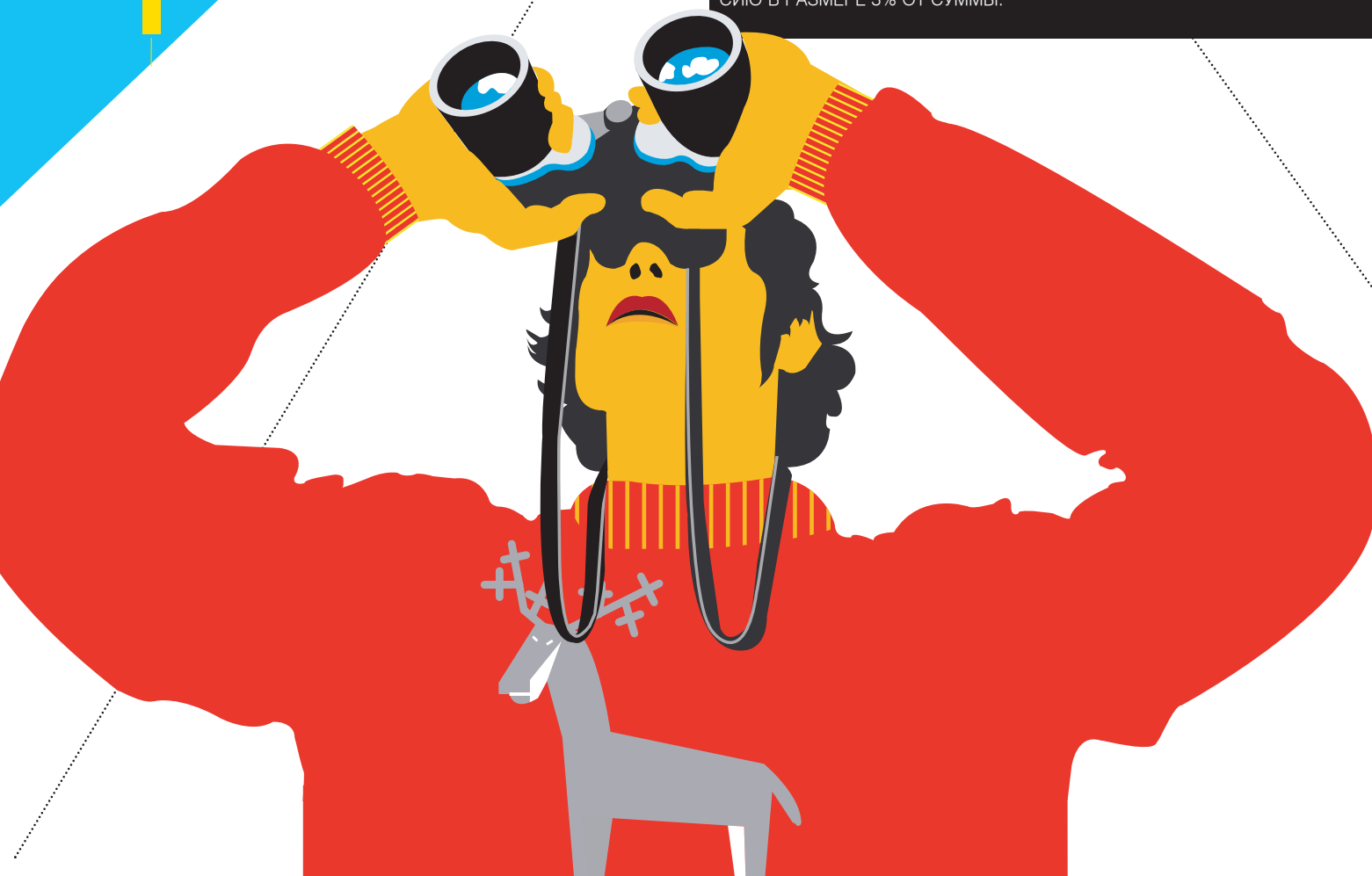
«ЯНДЕКС.ДЕНЬГИ»

РЕГИСТРИЦИЯ В «ЯНДЕКС.ДЕНЬГИ» ЕЩЕ ПРОЩЕ, ЧЕМ В WEBMONEY. С НЕДАВНИХ ПОР ДЛЯ РАБОТЫ В СИСТЕМЕ НЕ ТРЕБУЕТСЯ УСТАНОВЛИВАТЬ НИКАКОЙ СПЕЦИАЛЬНЫЙ СОФТ НА КОМПЬЮТЕР. ВСЕ ДЕЛАЕТСЯ ЧЕРЕЗ WEB-ИНТЕРФЕЙС. ДЛЯ АКТИВАЦИИ КОШЕЛЬКА НЕОБХОДИМО ЗАРЕГИСТРИРОВАТЬСЯ В ОДНОМ ИЗ ПРОЕКТОВ ЯНДЕКСА, НАПРИМЕР НА ПОЧТЕ. ДАЛЕЕ ЗАЙТИ НА <http://money.yandex.ru> И ПЕРЕЙТИ ПО ССЫЛКЕ «АКТИВИЗИРОВАТЬ КОШЕЛЕК». ЗАТЕМ ВНИМАТЕЛЬНО ЗАПОЛНИТЬ ФОРМУ РЕГИСТРАЦИИ И НАЖАТЬ КНОПКУ «СОХРАНИТЬ». ОБЯЗАТЕЛЬНО ЗАПОМНИТЬ ПЛАТЕЖНЫЙ ПАРОЛЬ — БЕЗ НЕГО НЕ ПОЛУЧИШЬ ДОСТУПА К КОШЕЛЬКУ. ЕСЛИ ТЫ ЗАПОЛНИЛ ВСЕ ПРАВИЛЬНО, УВИДИШЬ ПАНЕЛЬ УПРАВЛЕНИЯ КОШЕЛЬКОМ. РАЗОБРАТЬСЯ С НЕЙ НАМНОГО ПРОЩЕ, ЧЕМ С WM KEEPER, ПОЭТОМУ ВОЗДЕРЖИСЬ ОТ КОММЕНТАРИЕВ. ЗАПИШИ НОМЕР СЧЕТА: ВДРУГ КТО-НИБУДЬ ЗАХОЧЕТ ПЕРЕЧИСЛИТЬ ДЕНЬГИ ПО ЭТОЙ СИСТЕМЕ ТЕБЕ.

ЧТОБЫ ВОСПОЛЬЗОВАТЬСЯ СИСТЕМОЙ, НЕ НУЖНО ОТКРЫВАТЬ СЧЕТ В БАНКЕ. ПРИ РЕГИСТРАЦИИ БУДЕТ ОТКРЫТ СЧЕТ, СВЯЗАННЫЙ С ТВОИМ КОШЕЛЬКОМ. ДЕНЬГИ НА ТВОЙ СЧЕТ МОГУТ ПОСТУПАТЬ ИЗ СЛЕДУЮЩИХ ИСТОЧНИКОВ:

- ОТ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ;
- ПОСРЕДСТВОМ БАНКОВСКОГО ПЕРЕВОДА;
- ПОСРЕДСТВОМ ПЕРЕВОДА С КРЕДИТНОЙ КАРТОЧКИ;
- ПОСРЕДСТВОМ ПОЧТОВОГО ПЕРЕВОДА. ЯСНО, ЧТО ПОПОЛНИТЬ СВОЙ СЧЕТ (ИЛИ СЧЕТ ДРУГОГО ПОЛЬЗОВАТЕЛЯ) МОЖНО В ОФИСЕ «ЯНДЕКСА», НО НЕ ДУМАЮ, ЧТО ЭТО УДОБНО ДЛЯ ВСЕХ.

РАБОТА В СИСТЕМЕ ОЧЕНЬ ПРОСТА. ТЫ ЗАРЕГИСТРИРОВАЛСЯ, ПОПОЛНИЛ СВОЙ СЧЕТ. ЗАХОДИШЬ В КАКОЙ-НИБУДЬ ИНТЕРНЕТ-МАГАЗИН, ПОДДЕРЖИВАЮЩИЙ «ЯНДЕКС.ДЕНЬГИ», И ВЫБИРАЕШЬ НУЖНЫЙ ТОВАР — НАЖИМАЕШЬ КНОПКУ «КУПИТЬ». ИНТЕРНЕТ-МАГАЗИН ПРИСЫЛАЕТ ТЕБЕ ДОГОВОР КУПЛИ-ПРОДАЖИ, КОТОРЫЙ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ МАГАЗИНА (ЧТОБЫ НИКТО ДРУГОЙ НЕ СМОГ ОТПРАВИТЬ ДОГОВОР ТЕБЕ ОТ ИМЕНИ МАГАЗИНА). ЧИТАЕШЬ ТЕКСТ ДОГОВОРА, И ЕСЛИ ТЫ СОГЛАСЕН И У ТЕБЯ ЕСТЬ НУЖНАЯ СУММА, ТО ОПРЕДЕЛЕННОЕ КОЛИЧЕСТВО ДЕНЕГ АВТОМАТИЧЕСКИ СНИМАЕТСЯ С ТВОЕГО СЧЕТА И НАПРАВЛЯЕТСЯ В КОШЕЛЕК ПРОДАВЦА. ОБ ЭТОМ СОБЫТИИ ТЫ ПОЛУЧИШЬ УВЕДОМЛЕНИЕ — КВИТАНЦИЮ, ИЛИ ДОКАЗАТЕЛЬСТВО СОВЕРШЕННОЙ ОПЛАТЫ. КАК ВИДИШЬ, ВСЕ ПОХОЖЕ НА WEBMONEY, ТОЛЬКО НАЗЫВАЕТСЯ ИНАЧЕ. КАК И В СЛУЧАЕ С WEBMONEY, ПРИ ЖЕЛАНИИ МОЖНО ОБМЕНЯТЬ «ЯНДЕКС.ДЕНЬГИ» НА ОБЫЧНЫЕ НАЛИЧНЫЕ, ПОЛУЧИТЬ КОТОРЫЕ МОЖНО ИЛИ В ОФИСЕ «ЯНДЕКСА», ИЛИ БАНКОВСКИМ ПЕРЕВОДОМ. ЗА ВЫДАЧУ ДЕНЕГ СИСТЕМА ВЗИМАЕТ КОМИССИЮ В РАЗМЕРЕ 3% ОТ СУММЫ.



ШАГ 1
ЗАХОДИШЬ НА
www.webmoney.ru
И СКАЧИВАЕШЬ
WEBMONEY KEEPER
CLASSIC

ШАГ 2
РЕГИСТРУЕШЬСЯ
В СИСТЕМЕ. НЕ-
СМОТЯ НА ТО,
ЧТО WEBMONEY
ДОПУСКАЕТ АНО-
НИМНОСТЬ, СВОЕ
ФИО УКАЗАТЬ НЕ
ПОМЕШАЕТ. ЕСЛИ,
КОНЕЧНО, ТЫ НЕ
ПЛАНИРУЕШЬ НЕМ-
НОГО «ПОХУЛИГА-
НИТЬ» С ЭЛЕКТ-
РОННОЙ НАЛИЧ-
НОСТЬЮ :)

задуматься о качестве интернет-соединения. Если оно оставляет желать лучшего, нужно организовать выделенку или хотя бы купить хороший модем. Например, «вездеход» ZyXEL U336 стоит около \$150, а б/у можно найти и за \$80, хотя те же 80 стоит новенький ZyXEL Omni.

После загрузки запусти скачанный файл, процедура установки пройдет без проблем, справишься без моих комментариев. Во время установки внимательно читай все сообщения, которые будет выводить программа.

Сразу после установки запусти WM Keeper (далее буду называть ее просто Кеерер). Смотрится довольно оригинально — прямо-таки «настоящий электронный сейф». Поскольку мы еще ни разу не регистрировались, нажать кнопку «Регистрация». Только перед этим не забудь установить соединение с интернетом.

Процесс регистрации довольно прост. Сначала нужно указать данные о себе: фамилию, имя, отчество, страну, город и электронный адрес (e-mail). E-mail указывать правильный, поскольку на него придет код для активации WM Кеерер.

Думаю, тебе не нужно в очередной раз напоминать, что пароль должен быть «серьезным», только не таким, что завтра ты забудешь его. В любом случае, в качестве пароля нельзя использовать qwerty, 123456, 1234567 (и т.д.), дату рождения, имена близких и прочую информацию, которая за полчаса подбирается злоумышленником, если он взламывает твой кошелек.

После указания всех данных начнется генерация файла ключей для доступа к твоему кошельку. Во время этого процесса старательно нажимай все клавиши на клавиатуре и со скоростью твоего

процессора перемещай указатель мыши по экрану — я не шучу. От твоей старательности зависит качество сгенерированного файла ключа.

После завершения генерации файла ключей Кеерер сообщит твой WMID — это твой идентификатор в системе WebMoney, его нужно записать. Также Кеерер сообщит, где находятся твои файлы ключей, без них ты не сможешь получить доступ к кошельку, одного пароля для этого недостаточно. Я рекомендую сделать следующее. Сохранить свой WMID в каком-нибудь файле, затем записать на болванку этот файл (скрывать от посторонних его не стоит — это не секретная информация) и файлы ключей. Болванку спрятать в надежном месте (главное — не забыть потом, где именно). На дискету сохранять не нужно — уж больно они ненадежны.

Далее на твой e-mail, указанный при регистрации, высылается код активации кошелька. Пока не введешь его, ты не сможешь пользоваться кошельком. Вот и все — установка завершена. Нажимаем кнопку «Готово».

Ты не получил код активации? Возможно, твой почтовый сервер принял письмо от робота WebMoney за спам, поэтому повтори всю регистрацию сначала, но укажи адрес своего провайдера — как правило, там не устанавливаются спам-фильтры. Если и это не помогло, обратись за помощью в службу поддержки — support@wmtransfer.com

после регистрации Перед тем как перейти к рассмотрению интерфейса, нужно подвести итоги регистрации. Итак, у тебя есть:

- ТВОЙ WMID.
- ФАЙЛЫ *.KWM И *.PWM — ЭТО СЕКРЕТНЫЕ ФАЙЛЫ. ПОСТАРАЙСЯ СДЕЛАТЬ ТАК, ЧТОБЫ ОНИ НЕ ПОПАЛИ В ЧУЖИЕ РУКИ.
- ЧЕТЫРЕ РАЗЛИЧНЫХ КОШЕЛЬКА, КОТОРЫЕ СВЯЗАНЫ С ТВОИМ WMID.

webmoney не для всех

ЛЮБОПЫТНЫЙ ФАКТ: МНОГИЕ СЕРВИСЫ WEBMONEY ТРЕБУЮТ АВТОРИЗАЦИИ KEEPER'A. ЭТО И БАНКИНГ, И ЦЕНТР АТТЕСТАЦИИ, И КРЕДИТНАЯ БИРЖА, И МНОГИЕ ДРУГИЕ. ВСЕ ХОРОШО. НО ДЛЯ АВТОРИЗАЦИИ KEEPER'A НУЖНА ТЕХНОЛОГИЯ ACTIVEХ. СООТВЕТСТВЕННО, МЫ ПОЛУЧАЕМ ЗАВИСИМОСТЬ WEBMONEY ОТ БРАУЗЕРА ОДНОЙ ИЗВЕСТНОЙ ФИРМЫ. А ИМЕННО ОТ INTERNET EXPLORER. ПОЛЬЗОВАТЕЛИ FIREFOX, MOZILLA И OPERA МУЧАЮТСЯ... ТО ЕСТЬ ДЛЯ ПОЛЬЗОВАНИЯ WEBMONEY ИМ ПОСТОЯННО ПРИХОДИТСЯ ЗАПУСКАТЬ IE, БОЛЕЕ ТОГО, НЕРЕДКО, СДЕЛАВ ПОКУПКУ В ИНТЕРНЕТ-МАГАЗИНЕ С ПОМОЩЬЮ WEBMONEY, ПРОЙДЯ РЯД ШАГОВ, ОНИ НАТЫКАЮТСЯ НА ЗАПРОС АВТОРИЗАЦИИ. А ЧЕРЕЗ АЛЬТЕРНАТИВНЫЕ БРАУЗЕРЫ ЭТО НЕВОЗМОЖНО. НЕ САМЫЙ ВЕСЕЛЫЙ РЕЗУЛЬТАТ, СОГЛАСИСЬ. РЕШЕНИЕ ЭТОЙ ПРОБЛЕМЫ СУЩЕСТВУЕТ. НУЖНО ЛИБО СКАЧАТЬ СПЕЦИАЛЬНЫЕ ПЛАГИНЫ ДЛЯ АЛЬТЕРНАТИВНЫХ БРАУЗЕРОВ, ЛИБО ЗАСТАВИТЬ ИХ В ОПРЕДЕЛЕННЫЕ МОМЕНТЫ ИСПОЛЬЗОВАТЬ ДВИЖОК IE, ТЕМ САМЫМ ЭМУЛИРУЯ ЕГО РАБОТУ. ПОДРОБНЕЕ ОБ ЭТОМ ТЫ МОЖЕШЬ ПОЧИТАТЬ НА ОЧЕНЬ ИНТЕРЕСНОМ И ПОЛЕЗНОМ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ WEBMONEY РЕСУРСЕ. НАЗЫВАЕТСЯ ОН КРАЙНЕ ПРОСТО — «О WEBМАНИ». ЕГО ТЫ МОЖЕШЬ НАЙТИ ПО ССЫЛКЕ www.owebmoney.ru/browsers.shtml

ШАГ 3

ПРИДУМАЙ ПАРОЛЬ! НЕ ПОЛЕНЫСЬ ЕЩЕ РАЗ ТЕБЕ НАПОМНИТЬ, ЧТО НЕ НАДО ИСПОЛЬЗОВАТЬ QWERTY В КАЧЕСТВЕ ПАРОЛЯ! САМОЕ УЯЗВИМОЕ МЕСТО ПРИ КРАЖЕ E-MONEY — ЭТО САМ ПОЛЬЗОВАТЕЛЬ

ШАГ 4

СОХРАНИ ПОЛУЧЕННЫЙ WMID В КАКОМ-НИБУДЬ ФАЙЛЕ, ЗАТЕМ ЗАПИШИ ЕГО И ФАЙЛЫ КЛЮЧЕЙ НА CD. БОЛВАНКУ СПРЯТАТЬ В НАДЕЖНОМ МЕСТЕ (ГЛАВНОЕ — НЕ ЗАБЫТЬ ПОТОМ, ГДЕ ИМЕННО)

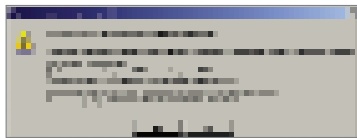
ШАГ 5

ПРОВЕРЬ E-MAIL, УКАЗАННЫЙ ПРИ РЕГИСТРАЦИИ — ТУДА ВЫСЛАН КОД АКТИВАЦИИ. ПРОЙДИ ПО ССЫЛОЧКЕ... ПОЗДРАВЛЯЕМ: ТЫ — ПОЛНОЦЕННЫЙ ПОЛЬЗОВАТЕЛЬ СИСТЕМЫ WEBMONEY

сверху вниз:

Запиши свой WMID
Добавление сертификата: обязательно нажать «Да» (Yes)

Если с WMID и ключами все ясно, то с кошельками не очень. После регистрации система автоматически создает четыре электронных кошелька: Z-кошелек, R-кошелек, U-кошелек и E-кошелек. Что такое кошелек в реальной жизни, мы знаем: это нечет, в чем хранят деньги. Электронный кошелек — это кошелек для хранения электронных денег. Для работы в WebMoney необходим хотя бы один кошелек, вообще число кошельков не ограничено: позже ты сможешь создать несколько кошельков, например два дополнительных Z-кошелька. На один из них будут поступать деньги из твоего интернет-магазина, на другой — деньги от покупателей твоих программ, на третий — все остальное, что не попало в первые два. Фильтрации никакой нет, ты сам определяешь, кому предоставить номер кошелька и какой из имеющихся. Номер кошелька похож на номер счета в банке. Например, на сайте интернет-магазина ты указал один кошелек, а заказчиком прислал по почте совершенно другой кошелек. Поскольку кошельки связаны с WMID, система знает, что эти деньги именно твои, а не Иванова или Петрова.



Z-кошельки предназначены для хранения долларов США. В этом кошельке хранятся деньги, которые для удобства называют WMZ. 1 WMZ = 1 USD — как видишь, все прозрачно и просто. Номер Z-кошелька состоит из буквы Z (это тип кошелька) и 12-ти цифр. Номер моего Z-кошелька —

Z175522617416. Без Z указывать его нельзя, иначе система не воспримет номер. Если я хочу, чтобы кто-то перечислил деньги на мой кошелек, я должен сообщить ему этот номер — Z175522617416. Помни, что номер кошелька никогда не совпадает с номером WMID. Кошельков может быть много, а WMID один.

Аналогично, в R-кошельке хранятся рубли, но они здесь называются WMR. Курс такой: 1 WMR = 1 RUR. Номер R-кошелька состоит из буквы R и 12-ти цифр, следующих за ней, например R147575447668.

В E-кошельке хранятся евро. Принцип нумерации такой же: E334546931180. Курс тоже неизменный: 1 WME = 1 евро. U-кошелек предназначен для хранения электронных гривен (для тех, кто не знает, это украинская валюта). 1 WMU = 1 UAH.

Все операции в системе можно производить с кошельками одного типа. Предположим, у тебя есть деньги на Z-кошельке. Ты можешь отправить их только на Z-кошелек, но не можешь отправить их на кошелек другого типа. Если же нужно сделать это, ты должен обменять деньги (как в обычном обменном пункте), например с WMZ на WMU по внутрисистемному курсу. Деньги будут записаны на твой WMU-кошелек, а с твоего WMZ-кошелька — будут сняты. Думаю, все ясно. Были доллары, стали гривны. Теперь WMU-деньги можно отправлять на U-кошелек.

Нужно отметить, что самым популярным является Z-кошелек. Наверное, наши граждане привыкли к вечнозеленой валюте. Но это ни в коем случае не означает, что другие типы кошельков второсортные — все они равнозначны в системе.

интерфейс программы

Если Кеерер открыт, закрой его — начнем с самого начала. Теперь запусти его снова и нажми кнопку «Вход». Кеерер попросит тебя ввести твой WMID и пароль. После этого запустится основное окно Кеерер'a. Окно Кеерер'a не отображается на панели задач. Если ты переключишься на другое окно, для активизации Кеерер'a щелкни на его пиктограмме в системном трее. Кстати, эта пиктограмма изменяется в зависимости от состояния Кеерер'a.

Теперь вернемся к основному окну программы. Интерфейс программы очень удобен, прост и разговаривает на русском. Думаю, он не нуждается в особых комментариях. Слева находятся четыре закладки (сверху вниз): «Корреспонденты», «Описания покупок», «Кошельки», «Информация». В первом разделе («Корреспонденты») находится информация обо всех пользователях, с которыми ты имел дело: или перечислял им деньги, или они — тебе.

ШАГ 6

МЕНЮ КЕЕРЕР'А ДОНЕЛЬЗЯ ПРОСТОЕ, А ИНТЕРФЕЙС ИНТУИТИВНО ПОНЯТЕН, АБСОЛЮТНО ВСЕ ФИНАНСОВЫЕ ОПЕРАЦИИ СО СВОИМИ НОВЫМИ ЭЛЕКТРОННЫМИ ДЕНЬГАМИ СОВЕРШАЙ ЧЕРЕЗ ГЛАВНОЕ МЕНЮ ПРОГРАММЫ



ШАГ 7

СОБСТВЕННО, ЭТОГО ШАГА И НЕТ. ПРОСТО ДЕЛАЙ ВСЕ ТО, ДЛЯ ЧЕГО ТЫ И ЗАВОДИЛ ЭЛЕКТРОННЫЕ ДЕНЬГИ. МОЖЕТ БЫТЬ, ЭТО ДАЖЕ НАПРЯМУЮ СВЯЗАНО С ШАГОМ 2 :)

Второй раздел пока не нужен, разберешься с ним чуть позже. В третьем разделе содержатся сведения о твоих кошельках. В последний раздел можно зайти, когда у тебя будет время разобраться с WebMoney подробнее, — там содержится информация о самой WebMoney. Кнопка меню вызывает основное меню Кеерер'a.

Все финансовые операции (и не только финансовые) ты можешь осуществлять с помощью основного меню. Предположим, ты хочешь отправить кому-то деньги. Выбери «Меню» > «Кошельки» > «Передать WM» > в кошелек WebMoney. Обрати внимание на то, что здесь же ты можешь передать деньги в какой-нибудь банк, например на чью-то кредитную карточку. В открывшемся окне все ясно: выбираем свой кошелек, вводим сумму, которую нужно отправить, вводим номер кошелька и нажимаем кнопку «Передать».

Ясно, что если у тебя нет нужной суммы денег, то и перечислить ее невозможно. Если ты читал статью об электронных деньгах, то должен был запомнить, что такое сделка с протекцией (защитой). Протекция используется в случаях:

- КОГДА ТЫ НЕ УВЕРЕН, ЧТО ПОЛУЧИШЬ ТОВАР. УСТАНОВИ ЧИСЛО ДНЕЙ ЗАЩИТЫ (ПРИБЛИЗИТЕЛЬНОЕ ЧИСЛО ДНЕЙ, В ТЕЧЕНИЕ КОТОРЫХ ТЫ РАССЧИТЫВАЕШЬ ПОЛУЧИТЬ ТОВАР) И КОД ПРОТЕКЦИИ (ЧТО-ТО ВРОДЕ ПАРОЛЯ; ЛЮБАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ СИМВОЛОВ). ЕСЛИ ТЫ ПЕРЕВОДИШЬ ДЕНЬГИ С КОДОМ ПРОТЕКЦИИ, ТО ПОЛУЧАТЕЛЬ ДОЛЖЕН УЗНАТЬ ОТ ТЕБЯ КОД ПРОТЕКЦИИ. ЕСЛИ ЖЕ ПРОТЕКЦИЯ НЕ БУДЕТ СНЯТА В ТЕЧЕНИЕ УКАЗАННОГО ЧИСЛА ДНЕЙ, ДЕНЬГИ ВОЗВРАЩАЮТСЯ НА ТВОЙ КОШЕЛЕК. ЯСНО, ЧТО ТЫ СООБЩИШЬ КОД ПРОТЕКЦИИ ПОЛУЧАТЕЛЮ, КОГДА ПОЛУЧИШЬ ДЕНЬГИ.
- КОГДА ТЫ НЕ УВЕРЕН, ЧТО ПРАВИЛЬНО УКАЗАЛ НОМЕР ПОЛУЧАТЕЛЯ. СНОВА ТЫ СТРАХУЕШЬ САМОГО СЕБЯ. ИСПОЛЬЗУЙ ПРОТЕКЦИЮ — ОЧЕНЬ ПОЛЕЗНАЯ ШТУКА.

счета Предположим, ты хочешь выписать кому-нибудь счет, например за написанную тобой программу. «Меню» > «Исходящие счета» > «Выписать». Введи WMID получателя, сумму, описание покупки и другую информацию — тут несложно, разберешься.

Если тебе пришел счет (об этом проинформирует пиктограмма Кеерер'a в системном трее), щелкни по пиктограмме Кеерер'a: откроется окно, в котором ты можешь оплатить счет или отказаться сделать это.

КОШЕЛЬКИ В этом разделе ты можешь управлять своими кошельками — создавать и удалять их. Для создания нового кошелька щелкнуть правой кнопкой на рабочей области и из появившегося меню выбрать команду «Создать». Осталось выбрать тип кошелька и ввести его описание, например «Кошелек для интернет-магазина».

КАК ПОПОЛНИТЬ СВОЙ СЧЕТ? Масса вариантов! Рассмотрим только основные варианты поступления денег на твои кошельки (подробнее ты узнаешь на сайте www.webmoney.ru):

- ЕСТЕСТВЕННЫМ ПУТЕМ — ОТ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ.
- ЧЕРЕЗ СБЕРБАНК — ТЫ САМ (ИЛИ КТО-ТО ДРУГОЙ) МОЖЕШЬ ПОПОЛНИТЬ СВОЙ КОШЕЛЕК ЧЕРЕЗ ЭТОТ БАНК.
- БАНКОВСКИЙ ПЕРЕВОД.
- С ПОМОЩЬЮ WM-КАРТ. ПОДРОБНЕЕ СМОТРИ ЗДЕСЬ — <http://webmoney.ru/cardmain.shtml>.
- ЧЕРЕЗ ДИЛЕРОВ СИСТЕМЫ WEBMONEY (https://dealer.webmoney.ru/asp/default_r.asp ДЛЯ РОССИИ ИЛИ https://dealer.webmoney.ru/asp/default_u.asp ДЛЯ УКРАИНЫ).

Дополнительную информацию о платежной системе WebMoney ты можешь найти на официальном сайте (www.webmoney.ru).

«деньги@mail.ru»

ЛЮБОПЫТНО, ЧТО НЕСМОТРЯ НА ТО, ЧТО РОССИЙСКИЙ РЫНОК ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ ПРАКТИЧЕСКИ СФОРМИРОВАН И ОСНОВНЫЕ ИГРОКИ НА НЕМ ОПРЕДЕЛЕННЫ, НА НЕГО ПОСТОЯННО УСТРЕМЛЯЮТСЯ НОВЫЕ КОМПАНИИ. ТАК, НЕДАВНО ПОЧТОВАЯ СЛУЖБА MAIL.RU ОБЪЯВИЛА О ЗАПУСКЕ СОБСТВЕННОЙ ЭЛЕКТРОННОЙ ПЛАТЕЖНОЙ СИСТЕМЫ — «ДЕНЬГИ@MAIL.RU». АДРЕС СИСТЕМЫ ОЧЕВИДЕН — money.mail.ru. НА ЭТОЙ СТРАНИЧКЕ ТЫ НАЙДЕШЬ ПОДРОБНУЮ ИНФОРМАЦИЮ О НОВОЙ СИСТЕМЕ. ПРИМЕЧАТЕЛЬНО, ЧТО, ПОМИМО ТОГО, ЧТО САМА MAIL.RU ОЧЕНЬ ПРИЛИЧНАЯ КОМПАНИЯ, ТАК ЗА ПРОЕКТОМ ДЕНЬГИ@MAIL.RU СТОЯТ ДРУГИЕ ИЗВЕСТНЫЕ ИГРОКИ, НАПРИМЕР ИНВЕСТИЦИОННАЯ КОМПАНИЯ «ФИНАМ».

безопасность

ДОВЕРЯЙ, НО ПРОВЕРЯЙ
КРАЖА ЭЛЕКТРОННЫХ ДЕНЕГ
ЧЕЙ SAFE ЛУЧШЕ?
МОБИЛЬНЫЕ КОМПЬЮТЕРЫ
АНОНС
ПЛАТИТЬ ПРЕДОХРАНЯЯСЬ
СЛОЖНЫЙ СИМБИОЗ
КАРДИНГ ПО-НОВОМУ
АТАКА НА СМАРТ-КАРТЫ



доверяй, но проверяй

БЕЗОПАСНОСТЬ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

СТОИТ ЛИ ЗАВОДИТЬ ЭЛЕКТРОННЫЙ КОШЕЛЕК? ОБЕСПЕЧИТ ЛИ ОН ОЖИДАЕМЫЙ ОТ НЕГО КОМФОРТ И УДОБСТВО? НЕ БУДУТ ЛИ УКРАДЕНЫ НАШИ ДЕНЕЖКИ? КАКИЕ ПЛАТЕЖНЫЕ СИСТЕМЫ СУЩЕСТВУЮТ И ЧЕМ ОНИ ОТЛИЧАЮТСЯ ДРУГ ОТ ДРУГА? ВОПРОСОВ МНОГО, НО ВСЕ ОТВЕТЫ НАХОДЯТСЯ ПОД ЗАМКОМ... | КРИС КАСПЕРСКИ АКА МЫЩЪХ

предыстория Можно ли доверять электронным деньгам? Они чистойшей воды абстракция и лишь квантовый шум в проводах — ни погрызть, ни понюхать. Самое надежное для хранения капиталов — золото, серебро, бриллианты. Закопал в саду, и никто не сопнет :). Цветметы не горят в огне, не обесцениваются при дефолтах, только слишком накладно и вообще непрактично каждый раз откапывать их, чтобы пожевать чипсов или покурить. К тому же правительства всех стран не очень-то стремятся разделять золото с народом: «Раздать золото и бриллианты легко, но как потом прикажете править?»

Вот почему драгоценные металлы изымаются из оборота и заменяются на фиктивные денежные знаки, которые как бы обеспечены золотым запасом страны. «Как бы» — потому что обменный курс валют выражается не в метрической системе, а в условных единицах, то есть деньги как бы замыкаются сами на себя. Если бы на каждом червонце было написано, к примеру, «обеспечивается одним граммом золота», никакой инфляции не случилось бы. Так ведь нет! Червонец можно обменять в «Сбербанке» на золото (теоретически), но только по текущему «золотоносному» курсу рубля, который зависит от множества обстоятельств. К тому же, если правительству внезапно потребуются финансы, то золото нужно либо отвоевывать, либо добывать. И то, и другое — слишком хлопотно. А с бумажными деньгами достаточно просто: включил печатный станок и даже не заботишься о том, обеспечиваются ли казной новые банкноты. Америка превысила свое эмиссионное право в несколько раз, и доллар спасается от своего падения только верой в американский сценарий «светлого будущего». В любой момент он может либо упасть в цене либо выйти из оборота (евро уже наступает).

В общем, бумажные деньги ненадежны и лучше вкладывать свои сбережения в технику/недвижимость, а доллары/рубли использовать как опе-



На схеме справа:
Участники типичной
платежной системы

интересные ссылки

www.dis.ru/fm/arkiv/2003/3/15.html — ДЕНЕЖНЫЕ РЕФОРМЫ В РОССИИ (КОЕ-ЧТО О ДЕНЬГАХ И ДРАГОЦЕННОСТЯХ).

www.marketing.spb.ru/lib-mm/sales/epay.htm — ВВЕДЕНИЕ В ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ (КОНЦЕПЦИЯ ТИПОВЫХ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ И ПРИНЦИП ИХ РАБОТЫ).

www.owebmoney.ru — САЙТ НЕЗАВИСИМОЙ СЛУЖБЫ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ WEBMONEY С КУЧЕЙ ПОЗНАВАТЕЛЬНЫХ СТАТЕЙ ПО WEBMONEY.

ративное средство товарно-денежного обмена. Забавно, что кеш-память и денежная наличность по-английски называются одинаково — *cache*.

пять причин недоразвитости Можно выделить несколько существенных моментов, которые по сути и сдерживают прогрессивное развитие электронных денег. Мы выделили пять таких моментов.

первая причина А что насчет электронных денег? Начнем с того, что юридический статус всех известных электронных платежных систем до сих пор не определен, а кража электронной наличности (даже в особо крупных размерах) не является «кражей» в уголовно-процессуальном смысле и не преследуется по закону. То есть преследуется, конечно, но не так строго, как кража бумажных денег. Вот и естественный соблазн поживиться. Возникает целая армия воинствующих хакеров, специализирующихся на виртуальных кражах. Разработчики электронных платежных систем настаивают на том, что защитные механизмы несокрушимы, а во всех кражах (уже принявших массовый характер) виноваты пользователи, которые не поставили/неправильно настроили брандмауэр, вовремя не обновили антивирус, не скачали свежий сервис-пак и т.д. Но пользователь и не подписывался в своем статусе эксперта по безопасности!

вторая причина Электронные кошельки, хранимые на жестких дисках или сменных носителях, в один миг могут быть уничтожены энтропией (сбоем операционной системы, аппаратным отказом и т.д.). Например, flash-брелок с кошельком одного пользователя съела собака. Чуткие сотрудники из службы поддержки (www.owebmoney.ru) разместили этот случай... в юморном разделе своего сайта. Им смешно, а у человека трагедия... Восстановить электронный кошелек в большинстве случаев все-таки возможно, но сколько времени и денег уйдет на это. Бумажные деньги, хранимые в банке (трехлитровой), по крайней мере не исчезают вдруг и бесследно. И собаки ими не питаются.

третья причина Единой платежной системы нет, а обмен деньгами между различными платежными системами до безобразия затруднен. Например, популярный на западе PayPal официально обслуживает только американцев, и оплата по PayPal из России вызывает большие проблемы. Перевести деньги с помощью нее, конечно, возможно, но вопрос в том, насколько это просто. В противном случае исчезает главное преимущество электронных денег — прозрачность и простота. А так и кредиткой воспользоваться можно.

четвертая причина Далеко не все участники рынка принимают электронные деньги к оплате. Например, одна фирма переводит зарплату на электронный кошелек, другая — нет. Какой-то провайдер принимает электронные деньги к оплате, какой-то — нет. Вообрази такую ситуацию: в карманах широких хакерских штанин — ни шиша, а на электронном кошельке есть некоторая наличность, но получатель платежа отвергает ее. Или ты заходишь в интернет-магазин. Наложный платеж есть, курьерская доставка есть, оплата по кредитке есть, а с электронными деньгами они еще не работают. Так что наличие электронных денег — еще не гарантия того, что удастся воспользоваться ими.

пятая причина Кстати про интернет-магазины. Если ты заказал наложенным платежом трехтомник Кнута, а

может ли webmoney исчезнуть?

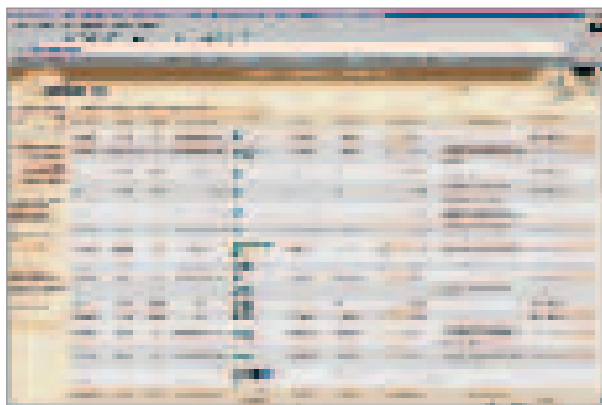
НЕ ЯВЛЯЮТСЯ ЛИ «ВЫЧИСЛИТЕЛЬНЫЕ СИЛЫ» ОЧЕРЕДНЫМ ЛОХОТРОНОМ НАПОДОБИЕ «МММ»? СИСТЕМА МУТНАЯ И ЗАПУТАННАЯ. НИКАКОЙ ПРОЗРАЧНОСТЬЮ ЗДЕСЬ И НЕ ПАХНЕТ. СПЛОШНАЯ ЧЕРНАЯ МГЛА. ДОКУМЕНТЫ НАПИСАНЫ ЯЗЫКОМ, ЧЕРЕЗ КОТОРЫЙ С ТРУДОМ ПРОДИРАЮТСЯ ДАЖЕ ПРОФЕССИОНАЛЬНЫЕ ЭКОНОМИСТЫ. СЛОЖНЫЕ ПРАВИЛА ВВОДА/ВЫВОДА ДЕНЕГ ИЗ СИСТЕМЫ. ЗАКРЫТЫЕ ПЛАТЕЖНЫЕ ПРОТОКОЛЫ.

ВСЕ ЭТО НЕ МОЖЕТ НЕ НАСТОРАЖИВАТЬ. СИСТЕМА СПРОЕКТИРОВАНА ОЧЕНЬ ХИТРО, СУДИ САМ: ЦЕНТРАЛЬНЫЙ ОПЕРАТОР В ЛИЦЕ «ВЫЧИСЛИТЕЛЬНЫХ СИЛ» ДЕКЛАРИРУЕТ WEBMONEY КАК СИСТЕМУ УЧЕТА ИМУЩЕСТВЕННЫХ ПРАВ. ГРУБО ГОВОРЯ, ОНА ГАРАНТИРУЕТ (ВИРТУАЛЬНЫМ ДОГОВОРОМ), ЧТО ЕСЛИ ТЫ ПОЛОЖИШЬ НА СВОЙ СЧЕТ ПЯТЬ ЕДИНИЦ, ОНИ НИКУДА НЕ ДЕНУТСЯ ОТТУДА. ЕСЛИ, КОНЕЧНО, ИХ НЕ УКРАДУТ.

ОПЕРАТОР НЕ ЗАНИМАЕТСЯ ОБНАЛИЧИВАНИЕМ ЭЛЕКТРОННЫХ ДЕНЕГ, ЭТО ПРЕРОГАТИВА ЕГО ПАРТНЕРОВ — ГАРАНТОВ, С КОТОРЫМИ У НЕГО ЗАКЛЮЧЕНЫ НЕКОТОРЫЕ СОГЛАШЕНИЯ. ОДНАКО ЛИЧНО ДЛЯ ТЕБЯ ГАРАНТЫ НИЧЕГО НЕ ГАРАНТИРОВАЛИ, НИКАКИХ ДОГОВОРОВ НЕ ЗАКЛЮЧАЛИ, И НИКАКИХ ОБЯЗАТЕЛЬСТВ ПЕРЕД ТОБОЙ У НИХ НЕТ. БОЛЕЕ ТОГО, ВИРТУАЛЬНЫЕ ЕДИНИЦЫ ПРИНАДЛЕЖАТ НЕ ИМ, А «ВЫЧИСЛИТЕЛЬНЫМ СИЛАМ», ПЛЮС ДЕНЬГИ, ВЫРУЧЕННЫЕ ОТ ИХ ПРОДАЖИ, ПЕРЕВОДЯТСЯ НА СЧЕТ «ВЫЧИСЛИТЕЛЬНЫХ СИЛ». САМ ГАРАНТ ПОЛУЧАЕТ ТОЛЬКО ПРОЦЕНТ, ТАК ЧТО ОН В ПРИНЦИПЕ НЕ МОЖЕТ НИЧЕГО ГАРАНТИРОВАТЬ — В ЕГО КАРМАНЕ НИЧЕГО НЕТ.

ЕСЛИ «ВЫЧИСЛИТЕЛЬНЫЕ СИЛЫ» ВДРУГ РАСТВОРЯТСЯ В ТУМАНЕ СО ВСЕМИ СВОИМИ БАНКОВСКИМИ СЧЕТАМИ ИЛИ ПРОСТО ПЕРЕСТАНУТ МЕНЯТЬ ЭЛЕКТРОННЫЕ ДЕНЬГИ НА НАЛИЧНЫЕ, ГАРАНТАМ ОСТАНЕТСЯ ТОЛЬКО РАЗВЕСТИ РУКАМИ. И С КЕМ ТЫ БУДЕШЬ СУДИТЬСЯ?! С «ВЫЧИСЛИТЕЛЬНЫМИ СИЛАМИ»? ТАК ТВОИ ЭЛЕКТРОННЫЕ ДЕНЬГИ ИСПРАВНО ЛЕЖАТ НА СЧЕТУ, И БЕРИ, ТРАТЬ — НЕ ХОЧУ! СУДИТЬСЯ С ГАРАНТАМИ? А ТЫ ЗАКЛЮЧАЛ С НИМИ КАКОЙ-ЛИБО ДОГОВОР? КАК ВАРИАНТ, «ВЫЧИСЛИТЕЛЬНЫЕ СИЛЫ» МОГУТ ПРОСТО ИЗМЕНИТЬ УСЛОВИЯ ВЫВОДА ДЕНЕГ: СТАНУТ ОБНАЛИЧИВАТЬ ТОЛЬКО СУММЫ ОТ \$100 000 И ВЫШЕ ИЛИ МНОГОКРАТНО ПРЕВЫСЯТ СВОЕ ЭМИССИОННОЕ ПРАВО, ТО ЕСТЬ ВЫПУСТЯТ ЕДИНИЦЫ, НЕ ОБЕСПЕЧЕННЫЕ НИКАКИМИ ДЕНЬГАМИ... ЗНАКОМЫЕ ЭКОНОМИСТЫ В ЧАСТНОЙ БЕСЕДЕ ЗАМЕЧАЛИ, ЧТО WEBMONEY ИДЕАЛЬНО ПОДХОДИТ ДЛЯ ПОДОБНОЙ МАХИНАЦИИ (В ПРОСТОРЕЧИИ «ДЛЯ АФЕРЫ»). ТАК ЧТО ДЕЛАЙ ВЫВОДЫ И МОТАЙ НА УС. А ЕЩЕ ПОМЕНЬШЕ ВЕРЬ ВСЯКОЙ ПРОПАГАНДЕ И УЧИСЬ ЧИТАТЬ МЕЖДУ СТРОК.

Обменный курс на электронной бирже часто устанавливается «по договоренности»



вместо него получил кирпич, можно просто не брать данное керамическое изделие, а дать им по голове курьера. В данной ситуации продавцу просто не резон обманывать покупателей, но при оплате электронными деньгами жульничество встречается сплошь и рядом. Даже кирпича не

KEEPER LIGHT ОСУЩЕСТВЛЯЕТ ВСЕ РАСЧЕТЫ ЧЕРЕЗ БРАУЗЕР

«АТТЕСТАТ ПСЕВДОНИМА» ВЫДАЕТСЯ АВТОМАТИЧЕСКИ ПОСЛЕ РЕГИСТРАЦИИ В СИСТЕМЕ

пришлют — просто покажут палец. Существует железное оправдание: «Кража электронной наличности» — вообще-то не кража». Владельца магазина, который работает с электронной наличностью, отмажет любой адвокат. Документов, подтверждающих перевод (пригодных для суда), у потерпевшей стороны все равно нет, а отследить получателя платежа нереально.

Для итога можно сказать, что электронные деньги при всей перспективности идеи еще не встали с горшка, до ясельной группы им еще расти и расти. Они не обеспечивают ни удобства, ни прозрачности, ни универсальности, ни надежности оплаты. Верить им нельзя! Однако пользоваться ими, пожалуй, можно :). Хотя бы в порядке эксперимента. Иметь пару кошельков с небольшими суммами для оперативных расчетов никогда не помешает, по крайней мере, потому что какой-то конкретный товарищ может предложить расчет только по WebMoney или все другие способы оплаты окажутся еще менее приемлемыми.

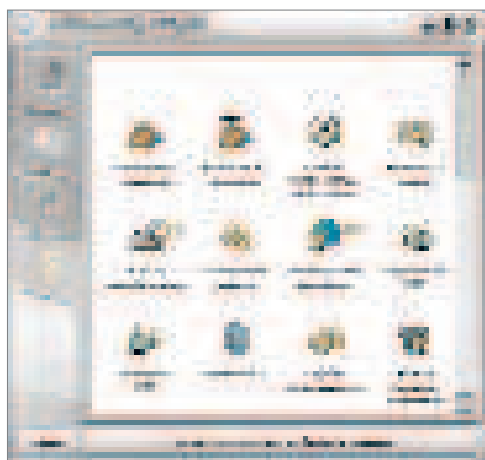
Чтобы не попасть впросак, необходимо ознакомиться с системой WebMoney извне и изнутри, чем сейчас и займемся.

электронные платежные системы При всем многообразии электронных платежных систем, присутствующих на рынке, они имеют некоторые общие черты. В каждой системе есть как минимум плательщик (payer) и получатель (payee). Перемещение денег от плательщика к получателю обеспечивается определенной последовательностью действий — протоколом электронного платежа. Теоретически обе стороны могут связываться и напрямую (современный криптографический аппарат позволяет это), но практически такая схема оказывается ненадежной и приходится вводить так называемые «финансовые институты», которые соотносят электронный перевод с реальным перемещением денежных средств. В роли «финансового института» могут выступить и банк, и любая другая уважаемая контора, которой доверяют участники обмена. Кстати, банки очень настороженно относятся к рискованным экспериментам с виртуальной наличностью. В основном финансовыми институтами становятся сами разработчики платежных систем, которые в принципе не способны обеспечить все электронные единицы живыми деньгами. Налицо превышение эмиссионного права в миллионы раз! Чтобы хоть как-то сгладить углы и удержать систему от падения, привлекаются дополнительные игроки...

Финансовый институт, принимающий денежные средства от плательщика, называется эмитентом (issuer). Институт, передающий их получателю, — эквайр (acquirer). Эмитент и acquirer могут осуществлять перевод любым платежным протоколом (грузить апельсины бочками) или даже быть единым и двуликим Янусом, обслуживающим и плательщиков, и получателей.

Если Янус один, платежная система называется централизованной, что, во-первых, означает постоянный «перегруз» центрального сервера, во-вторых — подрыв доверия к системе (не приобретут ли все денюжки ноги в один прекрасный день?). Вот почему центральный финансовый институт обычно делегирует часть своих прав сторонним конторам, контролируя их деятельность или не контролируя. Контроль — это и плохо, и хорошо. «Хорошо», потому что центр в ответе за все: если эмитент смотался с чужими деньгами, их оплачивает «материнская» организация, а за самим эмитентом бегают Янус с паяльником. С другой стороны, в такой системе задавлена инициатива и отсутствует конкуренция, значит, спектр предоставляемых услуг невелик...

Если контроль отсутствует, работать с электронными деньгами может любой желающий. Добиваться одобрения «центра» необязательно, и потому можно вводить мыслимые и немыслимые услуги, лишь бы существовал спрос. Ценой за это становится отсутствие каких бы



Интерфейс программы Keeper Classic



Аттестат псевдонима опирается на сведения, которые пожелал сообщить пользователь

то ни было гарантий. Если тебя кинул «свободный Джо», можно обращаться только в прокуратуру, но добиваться возврата наличности от других участников рынка бессмысленно (хотя в условиях свободного рынка обязательно появятся лица, которые предложат услуги подобного рода, так что ситуация не совсем безнадежна).

В банковском мире действует первая схема. Центробанк зорко следит за всеми коммерческими банками и в случае малейших подозрений немедленно устраивает суровые разборки. А если банк, в который ты положил свои кровные, вдруг испарился без суда и следствия, все долги перебрасываются на Центробанк. По крайней мере, мы не останемся в одних трусах, но и спектр предоставляемых услуг остается на недоразвитом уровне, так как он контролируется Центробанком. Электронные платежные системы могут использовать либо первую, либо вторую схему, либо их комбинацию. Тогда на рынке будут присутствовать и «доверенные» конторы, и «серые» участники, которым люди доверяют только на свой страх и риск. Немного замороченно, но в жизни все еще сложнее и научиться пользоваться электронными платежами без ущерба для себя намного сложнее, чем приучить «форточки».

В любой платежной системе обязательно должен присутствовать арбитр (Arbiter) — независимое лицо, решающее спорные вопросы и питающееся за счет комиссионных сборов. Если в платежной системе арбитра нет или его «независимость» декларирована лишь условно, от такой системы лучше держаться подальше.

Платежи могут быть прямыми или косвенными. Прямой платеж подразумевает непосредственную связь плательщика с эмитентом и получателем, а получателя — с плательщиком и acquirer'ом. Плательщик передает получателю несколько тугриков, эмитент списывает эту сумму с его счета, acquirer начисляет ее на счет получателя. Классический пример прямого платежа — чек.

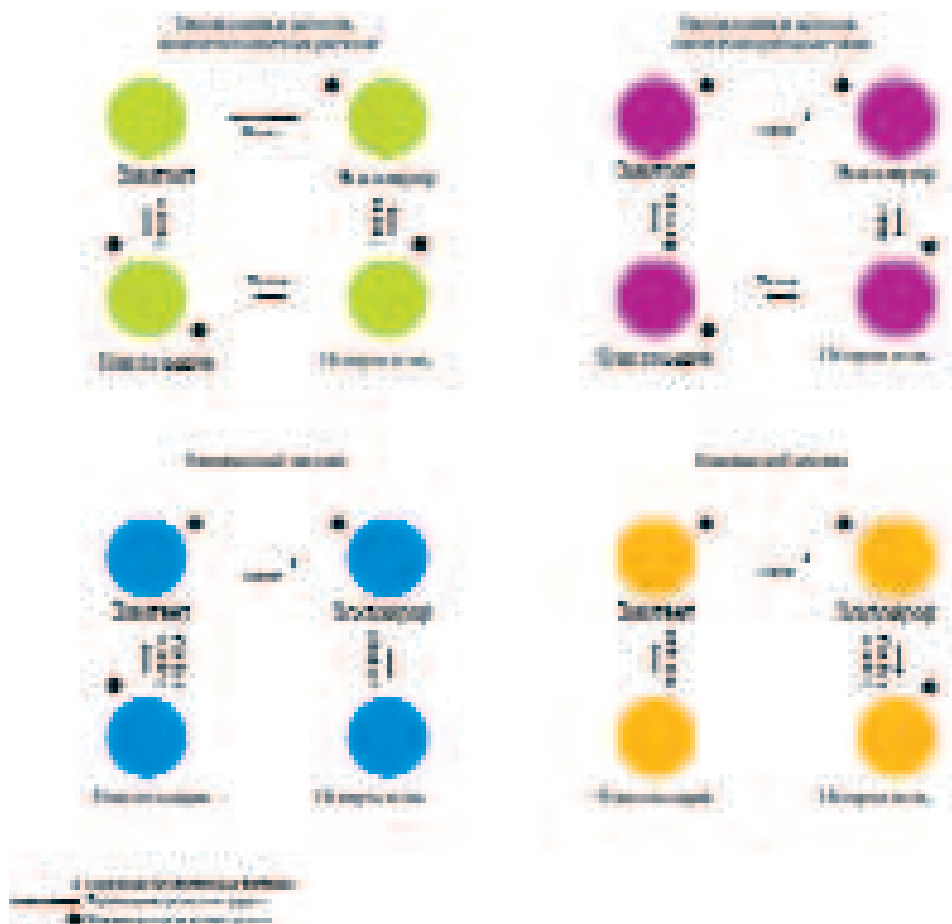
Существуют и косвенные системы, в которых плательщик связывается только с эмитентом, а получатель — только с acquirer'ом. Именно по этой схеме работает телеграфный перевод, для которого не требуется, чтобы обе стороны в момент оплаты находились в онлайн. К тому же косвенные системы защищены намного надежнее, чем прямые.

Большинство электронных платежных систем используют гибридную модель, чтобы унаследовать сильные стороны обеих схем и практически полностью ликвидировать их недостатки. Самый больной вопрос — безопасность. Электронная наличность может храниться как на центральном сервере владелицы платежной системы,

МНОГИЕ СЧИТАЮТ ИСПОЛЬЗОВАНИЕ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ СОМНИТЕЛЬНЫМ, ТАК КАК ТОЛКОМ НИЧЕГО О НИХ НЕ ЗНАЮТ

ОБМЕН МЕЖДУ РАЗЛИЧНЫМИ ПЛАТЕЖНЫМИ СИСТЕМАМИ ЗАТРУДНЕН, А ИНОГДА И ВОВСЕ НЕВОЗМОЖЕН

КРАЖА ЭЛЕКТРОННОЙ НАЛИЧНОСТИ ФОРМАЛЬНО НЕ ОПРЕДЕЛЕНА ЗАКОНОМ, ТО ЕСТЬ ОНА НАХОДИТСЯ ВНЕ ЗАКОНА



Прямые и непрямые платежи

предоставляя пользователям уникальный пароль (что-то вроде комбинации цифр от сейфа или связки ключей), так и непосредственно у самих участников платежа, например на smart-картах или в хитроумно зашифрованных файлах. С точки зрения безопасности, первый способ намного предпочтительнее: он максимально затрудняет генерацию фальшивых денег и в случае обнаружения кражи пароль на «сейфе» может быть быстро изменен, однако вернуть назад smart-карту уже невозможно.

Тем не менее, электронные деньги чрезвычайно уязвимы. Начнем с клиентского компьютера. Если хакер сумеет внедрить на него собственную программу, он запросто выгребет весь электронный кошелек подчистую. Также можно попытаться перехватить канал связи плательщика и получателя/эмитента, например запустить sniffer или взять под контроль один из промежуточных серверов. Впрочем, скорее всего это ничего не даст, так как протокол обмена изначально разрабатывается устойчивым к перехвату (во всяком случае, теоретически). А вот внедрение подложного эмитента может дать положительный результат! Его можно осуществить, например, путем «поднятия» DNS-сервера с последующим перенаправлением клиента на хакерский узел. Во многих платежных системах предусмотрена авторизация клиента сервером, но отсутствует авторизация сервера клиентом. Проще говоря, «игра идет в одни ворота». Чтобы подключиться к серверу, клиент должен знать некоторую уникальную информацию (грубо говоря, пароль), а сервер ничего не должен ему. И отличить «левый» сервер от «правого» в этом случае невозможно.

Наконец, можно взломать самого эмитента/асквирега — не так сложно, как может показаться на первый взгляд, особенно если в системе присутству-

ет множество независимых игроков, чьи серверы разрабатываются «на коленке». Представь, что произойдет, если банкоматы будут ставить не только банки, а все желающие. Появятся не просто банкоматы, а агрегаты, собранные и спроектированные по усмотрению его создателя. Даже если создатель «банкомата» честный инженер и никаких закладок там нет, вполне вероятно всплытие дыр.

Наконец, не стоит списывать со счета уже упомянутое мошенничество и простое попрошайничество. «Не дай обмануть себя в другом месте, покупай только у нас!». «Поддай на пропитание бедному голодному студенту. Мне срочно требуется операция по смене пола!» И т.п.

как устроена WebMoney

Количество существующих электронных платежных систем воистину огромно: Common Electronic Purse Specification (CEPS), European Electronic Purse (EEP), Mondex, Proton, Visa Cash, WorldPay, Globe ID Payment System, Millicent, NetBill, Mandate II, eCheck, BidPay, BillPoint, Q-Pass, i-Escrow, CyberCash, EDI Messages, Opening Buying on the Internet (OBI), Internet Open Trading Protocol, Java EC Framework и т.д. В России наиболее популярна WebMoney Transfer (далее для краткости — WebMoney), созданная московской компанией «Вычислительные Силы», корни которой уходят далеко за рубеж и теряются в штате Делавэр. Это довольно древняя система, она была создана еще в 1998 году, как раз во времена пресловутого кризиса, и за минувшее время охватила не только СНГ, но и более отдаленные страны. Система поддерживает рублевые, долларовые, евро- и гривновые кошельки. Самый популярный из них, естественно, долларовый.

Строго говоря, неправильно называть WebMoney «электронной платежной системой», так как это система учета имущества. Учет ведется в виртуальных единицах (условно они приравниваются к рублю, доллару, евро и гривне соответственно), которые находятся на счетах пользователей. Сама система обеспечивает только передачу единиц от одного пользователя к другому, а специальные финансовые институты («гаранты») обязуются выкупить (погасить) электронные единицы в момент требования. Поскольку юридический статус WebMoney до сих пор не определен, все гарантии сводятся к «честному слову» и «мамой клянусь». В общем, WebMoney функционирует лишь благодаря сложившемуся доверию к ней.

Центром системы является оператор (контора «Вычислительные силы»), который всего лишь предоставляет технические инструменты для учета (серверы и клиентское программное обеспечение), а ввод-вывод электронных денег из системы осуществляют ее партнеры — гаранты, за которых она несет моральную ответственность и не выбирает кого попало. Оператор контролирует финансовые операции внутри системы (переводы с одного кошелька на другой), а гаранты обеспечивают перевод электронной наличности в ту или иную валюту и наоборот.

посредники Помимо гарантов, в системе существует множество независимых игроков, например обменных пунктов, или, просто, «обменников». За чем они нужны? А затем, что планка минимальной суммы, которую можно перевести через гарант, с некоторых пор поднялась до... \$10 000 (подробности на <http://owebmoney.ru/bank-to-wmz.shtml>). Для большинства пользователей системы это, естественно, неприемлемо, поэтому гаранты и обзаводятся независимыми дилерами. С другой стороны, если ты получаешь зарплату в WebMoney, ты



Так выглядят карты оплаты WebMoney

разумно находишь знакомого, не вылезающего из интернет-магазинов, и обмениваешь WebMoney на доллары или рубли по своему собственному курсу. Если учесть, что обменники есть не везде, вполне вероятно, что для твоего знакомого будет выгоднее переплатить за электронные деньги на месте, а не ехать черт знает куда. Таким образом ты не только переведешь электронную наличность в твердые рубли, но и наживешься на этом!

Вывод денег из системы (то есть перевод электронных единиц в доллары или рубли) также очень заморочен и требует сложных телодвижений. «Официальный» сервис в лице <https://wire.exchanger.ru> предлагает выставить заявку, в ней указать свою контактную информацию и условия обмена, оплатить страховой взнос (2% от суммы) и ждать, пока кто-то не заинтересуется им. Встречная сторона тоже оплачивает страховой взнос и в течение двух дней осуществляет банковский перевод на счет получателя указанной суммы в затребованной валюте. После подтверждения успешности перевода через сайт exchanger'a электронный кошелек отправителя «автоматически» пополняется нужным количеством единиц (с вычетом комиссии 0,8%). В противном случае устраиваются серьезные разборки с привлечением администратора, который выступает «независимым» арбитром. Забавно. Не проще ли воспользоваться кредиткой? Воткнул в ближайший банкомат и получил свои зеленые. А тут... выставляя заявку, топай в банк...

Другой источник честной наживы — конвертация одного типа валюты в другой. Прямые операции между кошельками разных типов невозможны. Рубли всегда остаются рубликами, доллары — долларами, а евро — евриками (о гривне молчим :)).

Однако представим такую ситуацию. У нас есть долларовый кошелек, но получатель принимает платежи только в рублях. Как быть? Топать на биржу (<http://casher.ru>) или в ближайший обменный пункт. Может быть, у кого-то сложилась обратная ситуация: есть рублевый кошелек, но получатель хочет зеленых. Естественно, обменный курс у всех

свой (как говорится, «по договоренности»). На быструю и выгодную сделку лучше не рассчитывать, чтобы не разочароваться потом. Необходимо либо искать демократичный обменник, либо долго торчать на бирже, пока кто-нибудь не заинтересуется предложением. Но здесь исчезает главное преимущество электронных денег — простота и прозрачность использования.

безопасность и анонимность

Список проблем продолжается. Система WebMoney изначально спроектирована по методу «Что тут думать? Тут кодить надо и побыстрее». Для работы с электронными деньгами пользователю предлагается либо установить специальное программное обеспечение Keeper Classic, либо осуществлять все расчеты через браузер Keeper Light. Вопреки расхожему мнению, Keeper Light не использует ActiveX, то есть не является программой, а ограничивается одними «сертификатами», которые поддерживают практически все нормальные браузеры и под Windows, и под LINUX. Электронный кошелек в обоих случаях хранится в специальных файлах (.kwm/.pwm и .p12/.pfx), которые могут быть размещены и на сменном, и на постоянном носителе. Keeper Light плюс носитель с ключом обеспечивают доступ к кошельку из любого места, где только есть интернет. Как говорится, все свое ношу с собой! Правда, потребуются быстрый канал (Keeper Light просто пожирает трафик), а сервисные возможности будут весьма ограничены. Keeper Classic более функционален, но работает только с того компьютера, на котором был установлен, что не есть хорошо. Получаем электронный кошелек размером с компьютер! Хорошо, если у плательщика ноутбук... Таскать с собой десктоп весьма затруднительно :). Но вроде бы тоже без проблем: дома используешь Classic, во всех остальных местах — Light. Увы! Со своим кошельком можно работать только тем Кеерер'ом, в котором он был зарегистрирован. Кстати, восстановление доступа к своему кошельку в Classic Кеерер после переустановки операционной системы по силам только продвинутому пользователю... Где хранить файлы электронного кошелька, тоже не вполне понятно. Винчестер — не слишком надежное место. Он может отказать, любой хакер может стащить/уничтожить кошелек (впрочем, если хакер внедрился в систему, он все равно стащит его). Сменные носители также не очень надежды. Flash-брелки легко потерять,

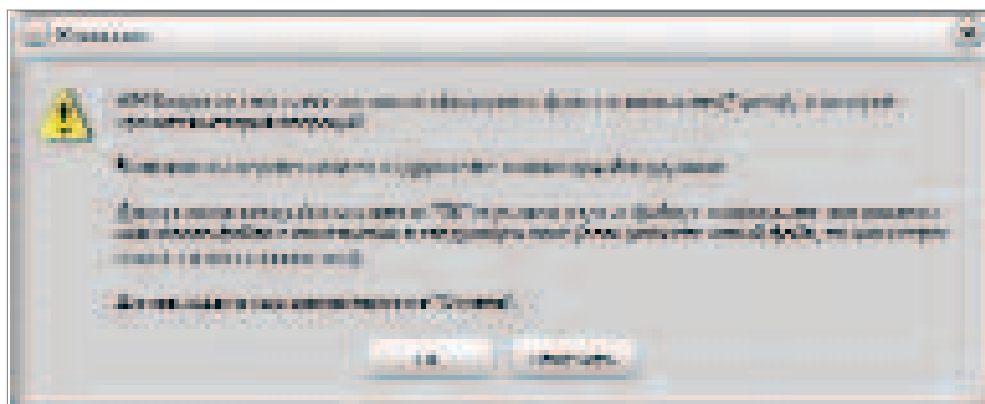
ОСНОВНАЯ ОПАСНОСТЬ ВЫТЕКАЕТ ИЗ ТОГО, ЧТО НЕ ВСЯ ЭЛЕКТРОННАЯ НАЛИЧНОСТЬ ОБЕСПЕЧЕНА РЕАЛЬНЫМИ ДЕНЬГАМИ

СПОРНЫЕ ВОПРОСЫ В ПЛАТЕЖНЫХ СИСТЕМАХ РЕШАЮТ НЕЗАВИСИМЫЕ АРБИТРЫ, КОТОРЫЕ ПОЛУЧАЮТ ЗА ДАННУЮ РАБОТУ КОМИССИОННЫЕ

ПОКА ЮРИДИЧЕСКИЙ СТАТУС WEB-MONEY НЕ ОПРЕДЕЛЕН, ВСЕ ГАРАНТИИ СВОДЯТСЯ К «ЧЕСТНОМУ СЛОВУ»

KEEPER CLASSIC РАБОТАЕТ ТОЛЬКО С ТОГО КОМПЬЮТЕРА, НА КОТОРОМ ОН БЫЛ УСТАНОВЛЕН

Реакция Keeper Classic на отсутствие файла *.pwm



болванки без толку занимают привод, дискеты сыплются и покрываются BAD-секторами без видимых причин... В общем, удобно, но все равно ненадежно.

И об анонимности. Это одновременно преимущество и проблема. Если кто-то ищет хакера для создания нового вируса, то обе стороны, естественно, хотят остаться в тени и осуществить перевод так, чтобы никто не знал, откуда он и куда. Но никаких гарантий, что оплата пройдет, естественно, не существует. Заберут вирус и покажут пальчик. Кого потом искать?! В обычной жизни анонимность платежей только создает проблемы. Именно по этой причине разработчики WebMoney придумали систему аттестатов — могучую, запутанную и криво работающую :). Раздачей аттестатов занимается Центр Аттестации (<http://passport.webmoney.ru>) и уполномоченные им лица (аттестаторы или регистры), которых насчитывается с полсотни.

аттестаты Существуют аттестаты различных уровней. «Аттестат псевдонима» выдается всем, кто регистрируется в системе. Формальный аттестат — всем, кто пожелал предоставить информацию о себе в Центре Аттестации. Начальный и Персональный аттестаты выдаются только за деньги (электронные) и только после проверки всех сведений Аттестатором. Как правило, требуют показать паспорт при личной встрече или выслать нотариально заверенное удостоверение. Стоимость аттестации колеблется от 5-ти до 20-ти долларов. Еще существуют аттестаты продавца/разработчика, регистратора, гаранта, оператора, но они менее интересны, поскольку мало кто пользуется ими.

Можно ли подделать аттестат? Чисто теоретически вполне возможно, так как это обычный сертификат, заверенный цифровой подписью. В данной области криптографы совершили прорыв еще лет пять назад, к тому же аппаратные мощности за последнее время значительно возросли, так что... Впрочем, можно пойти и по другому пути. Если сотрудники МВД неоднократно были замешаны в выдаче «левых» паспортов по непроверенным данным (статья!), то получить «нужный» аттестат можно куда за меньшее вознаграждение: с юридической точки зрения это не есть документ, и его «подделка», равно как и халатность, не будет сочтена преступлением при проверке регистрационных сведений. К тому же аттестаторы — не эксперты по безопасности, и закинуть на их компьютер программу, выдающую аттестаты от их имени, способен любой хакер. Достаточно просто вступить в переписку по e-mail, выцарапать из заголовка IP, запустить сканер безопасности и убедиться, что у них стоит незалатанная Windows с дырявым IE. А у некоторых даже находят целый табун заброшенных кем-то троянских коней :).

Аттестаты придуманы только для самоуспокоения и для честных людей. До тех пор, пока аттестат не будет признан юридическим документом (если когда-нибудь это время наступит, то нескоро), от виртуальных платежей лучше воздержаться. Риск нарваться на мошенника слишком велик, тем более что практически всегда можно найти альтернативные способы оплаты (наложенный платеж, кредитные карты и т.д.). Основное отличие кредитной карты от WebMoney состоит в том, что если по твоей кредитке будет сделана покупка, которую ты не совершал, с высокой степенью вероятности банк все-таки вернет деньги, а сотрудники WebMoney только разведут руками.

вердикт Очень часто пользователи системы WebMoney оказываются в ситуации: есть деньги, но нет возможности воспользоваться ими, а для платежной системы это фатально. Невозможность оплатить счет, быстро ввести или вывести деньги из системы равносильна их отсутствию. WebMoney требует глубокой начальной подготовки, которая опять-таки неприемлема для нефинансовых работников. Многие не хотят разбираться, как все это работает, кто такие обменники/биржи и где их искать. Человек имеет деньги и хочет совершить покупку, не вставая со своего кресла. Возможно ли это? В общем случае — нет и еще раз нет! Платежи через WebMoney имеют крайне ограниченную сферу применения и крайне небезопасны. Разработчики однозначно не знают, как создаются и взламываются защитные механизмы, поэтому кража электронных денег не представляет никакой проблемы. Опытный мошенник легко обчистит кошелек и в считанные минуты выведет деньги из системы так, что их будет не вернуть. Забавно, но WebMoney намного более дружелюбна к хакерам, чем к честным пользователям ;)

ЧИТАЙ В НОЯБРЕ:

МИРНЫМ ПОЛЬЗОВАТЕЛЯМ

ICQ.COM

КАК Я УДОБНО ИМУЮ ПРИБЛИЖИТЬСЯ К ТЕБЕ

ДЕДКА ДЛЯ ХАКЕРА

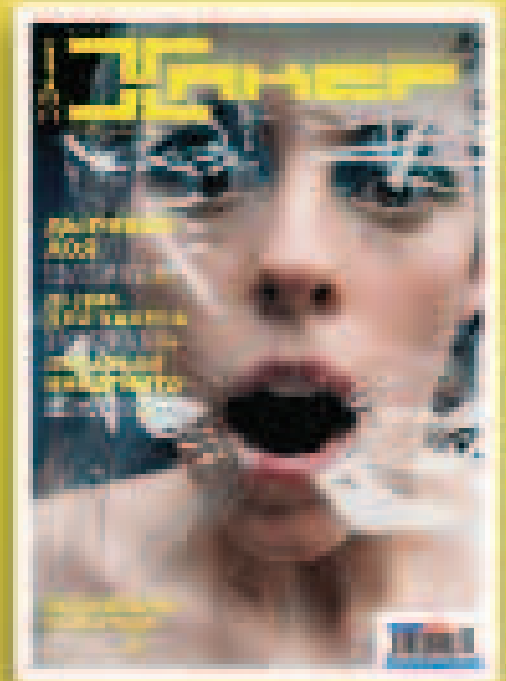
ВЫДАЧА ИМ ОБРАТНО-ОПЛАТ ДЛЯ ХАКЕРСКОГО ПРОЦЕССА

ПИРАТЫ XXI ВЕКА

КАК ПРАВИЛЬНО ПОДПИСАТЬСЯ ПРОИЗВОДИТЕЛЯ

САМОПАЛЬНЫЙ СЕРВИС

КОМУ НЕ ПЛАТЯТ ЗА СЕРВИС И КАК ЭТО РАБОТАЕТ



ПЛАТЯЩИХ ПИРАТАХ: ПИ ИЛИ НЕ ПЛАТЯЩИХ, ТОЛЬКО САМОМУ СЕБЕ НЕ ПЛАТЯТ ЗА СЕРВИС. А ТАКЖЕ ЗА ПИРАТСТВО



кража электронных денег

ВЗЛОМ И ЗАЩИТА WEBMONEY

ВОПРЕКИ ВСЕМ ЗАВЕРЕНИЯМ РАЗРАБОТЧИКОВ, СИСТЕМА WEBMONEY КАТАСТРОФИЧЕСКИ НЕНАДЕЖНА И ВСКРЫВАЕТСЯ БУКВАЛЬНО НОГТЕМ. СУЩЕСТВУЕТ МНОЖЕСТВО ЧЕРВЕЙ, ТРОЯНОВ И ХАКЕРСКИХ ГРУПП, СПЕЦИАЛИЗИРУЮЩИХСЯ НА ПОХИЩЕНИИ ЭЛЕКТРОННЫХ КОШЕЛЬКОВ, КРАЖИ КОТОРЫХ ПРИНЯЛИ МАССОВЫЙ ХАРАКТЕР | КРИС КАСПЕРСКИ АКА МЫШЦЬХ

Начнем с того, чего не может быть. Никаких «генераторов WebMoney» не существует и не может существовать. Вся наличность хранится на центральном сервере оператора, а электронные кошелки представляют собой лишь средство доступа к ней. Грубо говоря, если ты сгенерируешь комбинацию цифр для кодового замка, деньги и драгоценности в сейфе от этого не появятся. И хотя существует возможность подобрать шифр к чужому сейфу, вероятность открыть его без помощи владельца настолько мала, что об этом даже не стоит и говорить!

Украсть же чужую комбинацию вполне реально. Именно этим и занимаются «генераторы WebMoney», которые либо делают дубликат электронного кошелька и передают его злоумышленнику, либо скрыто вызывают Кеерег и осуществляют перевод на свой счет. Аналогичным образом действуют вирусы и троянские программы. Можно ли защититься от них?

Система WebMoney, разработанная неспециалистами, изначально проектировалась без оглядки на безопасность. Несмотря на то, что в последнее время появился целый комплекс «противопожарных» мер, прилепанных задним числом, положение остается критическим. Пользователи путаются в системах защиты, служба поддержки дает довольно туманные и расплывчатые рекомендации (обновить Windows, настроить брандмауэр и т.д.), а тем временем кражи электронных кошельков продолжают.

Мы не ставим перед собой задачу научить кого бы то ни было воровать, мы просто хотим показать и доказать (!), что система WebMoney действительно очень ненадежна и проектировалась даже не задницей (к ней все-таки примыкает спинной мозг), а неизвестно чем. Здесь не будет ни расплывчатых слов (чтобы нас не обвинили в клевете), ни конкретных рекоменда-

ций. Мы не даем готовых атакующих программ и не говорим, какие именно байтики нужно хакнуть, но гарантируем, что весь необходимый хакерский инструментарий может быть создан с нуля за одну ночь — святое для хакеров время!

начало, или классическая миссионерская

Система WebMoney — своеобразный аналог обыкновенных банковских чеков, следовательно, для совершения платежей в обязательном порядке необходимо предварительно зарегистрироваться на центральном сервере оператора и открыть счет, что уже является огромной неприятностью...

Идем на www.webmoney.ru, скачиваем программу Кеерег Classic, запускаем ее (так и не удалось заставить это чудо науч-

но-инженерной мысли работать через Proxy-сервер, пришлось поднимать NAT и маппить 2802-й порт), заполняем регистрационные данные (от фонаря или честно), придумываем себе любой пароль по вкусу, после чего программа приступает к генерации секретного ключа и просит подергать мышь и понажимать клавиши. Все это проделано ради получения действительно случайных данных —

ЧТО МОЖНО И ЧТО НЕЛЬЗЯ

ЭКСПЕРИМЕНТИРОВАТЬ (В ОБРАЗОВАТЕЛЬНЫХ ЦЕЛЯХ) МОЖНО ТОЛЬКО СО СВОИМ СОБСТВЕННЫМ ЭЛЕКТРОННЫМ КОШЕЛЬКОМ ИЛИ С КОШЕЛЬКАМИ ЛИЦ, ПРЕДОСТАВИВШИХ СООТВЕТСТВУЮЩЕЕ ПИСЬМЕННОЕ РАЗРЕШЕНИЕ :). НЕСАНКЦИОНИРОВАННОЕ ВМЕШАТЕЛЬСТВО В ЧУЖИЕ СИСТЕМЫ И КОШЕЛЬКИ КАТЕГОРИЧЕСКИ НЕДОПУСТИМО!

как будто псевдослучайный генератор на основе таймера здесь не годится. На фоне общей незащищенности системы бравировать словами RSA, RC5, MD4, MD5 и SSL просто глупо. Впрочем, психологический расчет разработчиков вполне понятен. Если секретный ключ будет генерироваться за доли секунды, какой пользователь в него поверит?

По завершении регистрации нам присваивается уникальный 12-значный идентификатор WMID (Web Money ID) и пара сгенерированных ключей. Открытый ключ передается на центральный сервер оператора WebMoney, а секретный сохраняется в файле с расширением *.kwm (Key of Web Money), который может быть расположен на жестком диске, сменном носителе или смарт-карте. Как видишь, обыкновенная несимметричная криптография типа PGP.

Плюс ко всему создается файл *.rwm, хранящий сведения о кошельках (текущий баланс, история операций и т.д.). В принципе он необязателен, так как вся информация расположена на центральном сервере оператора. Кеерег может работать и без PWM-файла, автоматически подгружая данные из Сети, правда, только за последние три дня. Собственно, KWM-файл тоже необязателен и его можно восстановить, для чего необходимо знать пароль, иметь доступ к почтовому ящику, указанному при регистрации, а также нотариально заверенное заявление, что ты не лось (подробнее об этом по ссылке www.owebmoney.ru/returnkey.shtml). Чисто теоретически, хакер может хакнуть твои денежки только на основе пароля, но практически — для него это слишком хлопотно и небезопасно.

Секретной информацией, регламентирующей доступ к кошельку, является один лишь kwm-ключ. WMID везде публикуется открыто, и это нормально. Зная WMID, можно узнать регистрационные данные пользователя, которые он пометил «открытыми», но нельзя определить номер его кошелька (кошельков).

Номер кошелька — это условно-секретная информация. Зная номер кошелька, ты не сможешь вытащить из него деньги, но сможешь выставить счет, заполнив поле «описание покупки» как можно более правдоподобно. Конечно, дурацкий способ, но есть некоторый шанс, что он пройдет. Пользователи, регулярно оплачивающие множество мелких счетов, постепенно привыкают не обращать внимания на них и проверяют графу «от кого» только при возникновении сомнений.

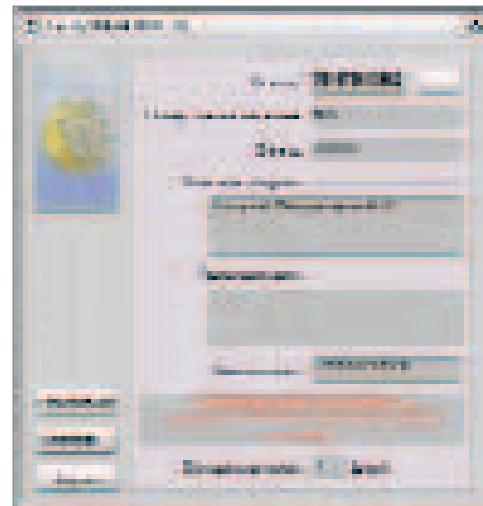
Кража KWM-файлов процветает. По умолчанию ключи сохраняются в keys.kwm, но в принципе имя файла может быть любым, как, впрочем, и расширение. Большинство хакеров и троянских программ производят тупой поиск по маске *.kwm, поэтому переименование файла ключей в dontreadme.txt до некоторой степени увеличивает защищенность. Однако продвинутые хакеры могут залезть в реестр, где Кеерег хранит свои настройки, и подсмотреть путь к файлу. Еще можно искать по его содержимому, сканируя все файлы (правда, это займет много времени и вызовет подозрительную дисковую активность). Гурманы наверняка перехватят вызов API-функции CreateFile, показывающей, какие файлы открывает Кеерег. И даже если формат настроек реестра в последующих версиях будет изменен, вариант с CreateFile продолжит работать. Хинт: если бы разработчики не были идиотами, они бы создали несколько файлов с ключами: один подлинный, все остальные — сторожевые датчики, при обращении к которым раздается сигнал тревоги :).

По умолчанию размер файла ключей составляет 1,2 Мб (на дискете), но при желании его можно увеличить вплоть до 100 Мб, что затруднит кражу ключа с передачей по интернету и не создаст никаких непреодолимых неудобств. 100 Мб — это половина mini CD-R, один Zip-100M или два CD-R в формате бизнес-карты. Конечно, быстродействие системы в некоторой степени упадет (огромный файл так сразу и не прочтешь), но безопасность стоит того. Или не стоит? Утащить 100 Мб по локальной сети — не проблема, по DSL-модему или кабельному интернету — тоже. И даже позорный по нынешним меркам модем на 33600 передаст этот файл за ~70 часов. Не так уж и много, если вспомнить, что практически никто из пользователей не регенерирует ключи каждый день. Разрезав файл на мелкие кусочки, передаваемые в фоновом режиме, вполне реально утащить его за две-три недели, хотя это будет самый тупой и неперспективный путь.

СИСТЕМА WEBMONEY ОЧЕНЬ ПОМОГАЕТ ПО ЖИЗНИ В СЕТИ, НО НЕ СТОИТ НЕДООЦЕНИВАТЬ ЕЕ УЯЗВИМОСТЬ

ПОСЛЕ РЕГИСТРАЦИИ КОШЕЛЬКА ЕМУ ПРИСВАИВАЕТСЯ 12-ЗНАЧНЫЙ ИДЕНТИФИКАТОР WMID (WEB MONEY ID)

СЕКРЕТНЫЙ КЛЮЧ ХРАНИТСЯ В ФАЙЛЕ *.KWM (KEY OF WEB MONEY)



Если хакер внедрился в чужую систему (а внедриться в нее можно разными путями), ему ничего не стоит загрузить файл в память, открыть кошелек, перевести деньги на свой счет и грохнуть жесткий диск, чтобы жертва не смогла войти в интернет и пожаловаться кому следует. Кстати, насчет «пожаловаться». Вариантов не так уж много, и помощи ждать неоткуда. Если у тебя еще есть доступ к WMID (что за тупой хакер попался?), можно определить WMID, на который были переведены деньги, зайти на сайт Арбитражного Сервиса (<http://arbitrage.webmoney.ru>), оплатить арбитражный сбор (а для этого необходимо иметь WebMoney, которых у нас подчистую умыкнул злоумышленник) и заблокировать хакерский кошелек.

Только если хакер не лось, деньги за считанные минуты будут переброшены на e-gold или выведены из системы любым другим путем, так что на его кошелек их не окажется и заблокировать будет особо нечего. Кстати, кошельки с начальным или персональным аттестатом блокируются только по решению арбитражной комиссии, то есть достаточно взять аттестат и... Только не надо думать, что владельцы аттестатов не занимаются воровством, поскольку сообщают свои паспортные данные. Выдачей аттестатов сейчас занимаются все кому не лень, и просто наивно надеяться, что все они люди честные, добросовестные и неподкупные. Тем более когда речь идет о деньгах, пусть даже электронных. Человек, который вознамерился похитить \$100 000 (а почему бы и нет?), без проблем получит не только фигурный аттестат, но еще и фальшивый паспорт в придачу. Даже если сотрудники МВД подделывают паспорта на потоке, о чем не раз говорило ТВ (а это уже криминал), то что говорить об «аттестатах», у которых вообще нет никакого юридического статуса.

Впрочем, разработчики все-таки рассмотрели ситуацию с переброской ворованных денег через несколько кошельков, и поэтому усердно позаботились о... злоумышленниках! Суди сам. После подачи уже упомянутого иска жертве следует обратиться к Администратору Арбитражного Сервиса (WMID 937717494180, arbitrage@webmoney.ru) и попросить его проследить цепочку. Вся «прелесть» в том, что Администратор работает только с понедельника по пятницу и с 10 до 18 часов по Москве, причем вывод денег из системы осуществляется практически мгновенно, поэтому счет идет на минуты.

Кстати, еще один вопрос: «Это студенческая общага или серьезная платежная система?» Что стоило при миллионных оборотах (о которых не перестает упоминать реклама) нанять несколько человек для круглосуточной поддержки? Речь в данном случае идет о деньгах! Естественно, для хакеров безопаснее всего совершать кражи либо в полночь, либо в выходные дни.

Выставляем жертве левый, но правдоподобный счет — а вдруг оплатит

что внутри кеерега Некоторые восхищаются тем, как разработчикам удалось втиснуть в объем Кеерега так много (опусы есть на www.owebmoney.ru/clashistory.shtml). А что они, собственно, в него вместили? Конечно, в наш век, когда Hello World с трудом вмещается на лазерный диск, программы, занимающие «все» несколько мегабайт, уже вызывают уважение :).

Основной объем (~2,2 Мб) занимает WMClient.dll, который, собственно, и есть Кеерег, он же DCOM-объект, написанный на Microsoft Visual .NET с компиляцией в машинный код, ничем не упакованный и никак не препятствующий своему анализу. Здесь нет ни шифрованного, ни р-кода, ни антиотладочных приемов, ни противодействия дизассемблеру, дамперу, API-шпиону. Ничего! Бери и анализируй. Во всяком случае, версия 2.4.0.3 (на момент написания статьи) ведет себя именно так. Будь разработчики хоть малость поумнее, они либо использовали бы Microsoft Visual C++ 6 (знаменитую «шестерку») плюс любой качественный протектор (например EхеCryptor), либо откомпилировали NET-приложение в р-код, дизассемблировать который намного сложнее.

WebMoney.exe (~180 Кб) — это только «пускалка», и в ней нет ничего интересного. Тем не менее, все-таки стоит дизассемблировать его. Хотя бы затем, чтобы посмеяться над разработчиками и оценить их квалификацию :).

как ломают кеерег Будем считать, что на компьютер с установленным Кеерегом внедрен хакерский код, исполняющийся с пользовательскими привилегиями. То есть условимся, что нам не дали администраторских прав, хотя повысить свои привилегии с «Пользователя» до system в W2K/XP в общем-то не проблема, не говоря уже о 9х, где никакого разделения привилегий отродясь не бывало. Будем действовать в спартанских условиях, приближенных к боевым :). Что мы можем сделать? У нас два пути. Предварительно дизассемблировать Кеерег, восстановить протокол обмена с сервером, дожидаться, когда будет вставлен носитель, на котором лежит секретный ключ, и... дальше фантазируй сам :).

Но ковыряться в Кеереге лениво. Дизассемблирование — это кропотливое дело, и на восстановление протокола обмена может уйти не одна неделя. Использование сниферов существенно сокращает этот срок, но меня все равно ломает. Гораздо проще и эффективнее воровать деньги руками самого Кеерега. Устанавливаешь шпион, который засекает клавиатурный ввод, дожидается ввода WMID или определяет его другими путями: WMID не является секретом ни для кого (первый способ в основном используется вирусами, второй хорош при целенаправленной атаке). Затем в один «прекрасный» момент (после 18 часов или в выходной день) отключается вывод на экран, запускается WebMoney.exe и путем эмуляции клавиатурно-мышинного ввода делается все, что угодно. Например, пополняется кошелек жертвы. А почему бы и нет? Мы же ломаем свой собственный кошелек, верно? Вот его и пополним! Мы же не бандиты, а честные хакеры :).

Техника эмуляции ввода подробно описана в «Записках мышьяка», электронную версию которой можно бесплатно сжевать с ftp-сервера nezu-mi.org.ru (доступен не круглосуточно). Так что не будем разводить демагогию и жевать резину по сто раз. Отметим лишь общий механизм.

Сначала нужно найти окно Кеерега вызовом функции FindWindow или EnumWindows и определить его дескриптор. Затем, используя EnumWindows, перечислить дочерние окна, принадлежащие элементам управления (кнопкам, строкам редактирования и т.д.). Посылая элементам управления разнообразные сообщения (с помощью функции SendMessage), их легко взять под свой контроль. Для отключения вывода — либо перехватить службы GDI (реализуется сложно, но действует на ура), либо расположить поверх Кеерега отвлекающее окно, например окно браузера с порнографической картинкой :). Да много всякого тут можно придумать.

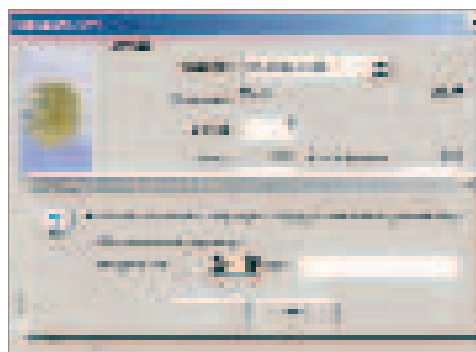
Проблема в том, что с некоторого времени тупая эмуляция перестала действовать. Кеерег обзавелся так называемыми «летающими цифрами»

Как ломают обменники

ВЗЛОМ ОБМЕННИКОВ НЕ ВХОДИТ В НАШИ ПЛАНЫ (СОБСТВЕННЫЙ ОБМЕННИК ИМЕЕТ ДАЛЕКО НЕ КАЖДЫЙ. А ЛОМАТЬ ЧУЖИЕ — НЕЗАКОННО), ПОЭТОМУ ОТМЕТИМ ЛИШЬ ОСНОВНОЕ. С ХАКЕРСКОЙ ТОЧКИ ЗРЕНИЯ ОБМЕННИК ПРЕДСТАВЛЯЕТ СОБОЙ САЙТ, ПРАВИЛЬНО УПРАВЛЯЕМЫЙ PHP И РАБОТАЮЩИЙ ПОД LINUX/BSD/NT. ИМЕННО ЧЕРЕЗ ОШИБКИ В PHP-СКРИПТАХ ИХ ЧАЩЕ ВСЕГО И ЛОМАЮТ. ТАКЖЕ НЕКОТОРЫЕ WEB-ПРОГРАММИСТЫ ОСТАВЛЯЮТ «ЧЕРНЫЙ ХОД» НА ТОТ СЛУЧАЙ, ЕСЛИ ИМ ВДРУГ ЗАХОЧЕТСЯ КУШАТЬ, А КУШАТЬ БУДЕТ НЕЧЕГО. РЕЖЕ ЛОМАЮТ ОСЬ. НАИБОЛЬШЕЕ КОЛИЧЕСТВО ДЫР, ЕСТЕСТВЕННО, ИМЕЕТ NT И ВСЕ ПРОИЗВОДНЫЕ ОТ НЕЕ СИСТЕМЫ (В ТОМ ЧИСЛЕ ХВАЛЕННЫЙ WINDOWS 2003 SERVER). ЧУТЬ СЛОЖНЕЕ СЛОМАТЬ LINUX И BSD, НО... ЕСЛИ ВЗЯТЬ СКАНЕР БЕЗОПАСНОСТИ (НАПРИМЕР X-SPIDER), ТО МОЖНО ОБНАРУЖИТЬ, ЧТО НА МНОГИХ ИЗ НИХ СТОИТ КОРЯВЫЙ SENDMAIL ИЛИ ПРОРЖАВЕВШИЙ APCACHE. ПЕРЕПОЛНЕНИЕ БУФЕРА, ЗАСЫЛКА SHELL-КОДА — И СЕРВЕР В ТВОИХ РУКАХ!

ОТ ПОТЕНЦИАЛЬНОЙ КРАЖИ ЭЛЕКТРОННЫХ ДЕНЕГ СПАСАЕТ ТОЛЬКО ИХ НЕИСПОЛЬЗОВАНИЕ

На этом примере Кеерег Classic в дизассемблере



Защита Кеерега «летающими цифрами»

являются на экране. Идея, конечно, интересная, но она позаимствована явно невпопад.

Почему «летающие цифры» действуют на web-серверах? Только потому что, во-первых, защитный код находится вне пределов досягаемости хакера, а во-вторых, потому что защита нацелена исключительно на роботов, а не на людей. Для охраны mail.ru от спамеров и вандалов такой меры более чем достаточно, а для Кеерега — решительно нет! В существующих версиях Кеерега летающие цифры элементарно распознаются простейшим OCR, а он свободно умещается в сотню килобайт (при использовании готовых библиотек). Хакерскому коду ничего не стоит захватить кусочек экрана и отправить его дежурящему у монитора хакеру, чтобы тот распознал их самостоятельно.

В-третьих, эта защита отключается бит-хаком, то есть правкой машинного кода Кеерега.



В-четвертых, летающие цифры можно вырубить через реестр (если попытаться отключить их средствами самого Кеерега, он запросит подтверждение на легитимность этой операции).

В-пятых, даже если защита будет ужесточена, в запасе у хакеров останется расшифровка протокола обмена и создание своих собственных клиентов без всяких там цифр.

В-шестых... Способов взлома очень и очень много, и никакой пользы от защиты «летающими цифрами» нет, не говоря уже о том, что многие пользователи до сих пор сидят на старых версиях без летающих цифр или отключают их за ненужностью.

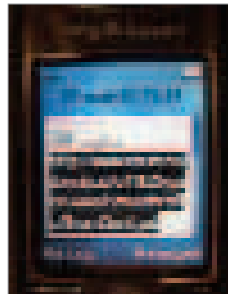
Еще одна широко разрекламированная фишка — подтверждение авторизации по мылу. На неискушенный взгляд, все выглядит железно: прежде чем сделать что-либо со счетом, вводишь код, код приходит на твое мыло. Если хакер упрет KWM-файл, он останется с носом, а владелец — с деньгами, так как злоумышленник не получил доступа к почтовому ящику. Логика железная, но неправильная :). Почтовые ящики ломаются (конкретные приемы взлома приведены во множестве книг и статей), к тому же хакер, утащивший KWM-файл, утащит и пароль на e-mail. Исключение составляет, пожалуй, лишь кража смарт-карт и сменных носителей с ключами. Но такая кража, как правило, осуществляется либо близкими людьми, которые могут поиметь и e-mail, либо грабителями, получившими физический доступ к сменному носителю, хранимому, как правило, в непосредственной близости от компьютера.

А как насчет блокировки всех IP-адресов, кроме своего? В локальных сетях захват чужого адреса не является непреодолимой проблемой. Тот же, кто сидит на Dial-Up'e, как правило, получает динамические IP-адреса, выделяемые из общего пула. Прописывать их развяжется пупок, да и любой клиент того же провайдера будет авторизован без проблем. И никакому хакеру не нужно хранить у себя чужой кошелек — проще снять деньги руками Кеерега, запущенного на компьютере жертвы, который наверняка имеет правильный IP, и никакая «блокировка» тут не спасет.

Защитные меры, предлагаемые разработчиками, можно перечислять очень долго. Практически все они ориентированы на воровство KWM-файла с последующей передачей по Сети. Почему-то разработчики думают, что это единственный способ взлома, и ошибаются. Еще они советуют «правильно» настроить брандмауэр, чтобы предотвратить утечку информации, и регулярно латать систему, чтобы не проникли ни хакеры, ни черви. Ну, насчет брандмауэров они явно погорячились. Достаточно сходить на популярный сайт www.firewallleaktester.com, чтобы убедиться в существовании атак, пробивающих все персональные брандмауэры.

Теперь разберемся с обновлениями. Многие сайты, принимающие оплату через WebMoney, работают только с IE, так как используют ActiveX. И хотя для

Последовательность операций при активации платежа через сотовый телефон или КПК

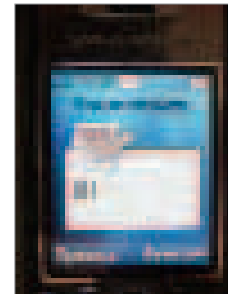


Активация платежа по сотовому телефону через систему ENUM

KEEPER LIGHT ЗАЩИЩЕН ХОРОШО, НО ПЛОХО ЗАЩИЩЕНЫ БРАУЗЕРЫ, ЧЕРЕЗ КОТОРЫЕ ОН РАБОТАЕТ

АВТОРИЗАЦИЯ С ПОМОЩЬЮ СОТОВОГО ТЕЛЕФОНА ЧЕРЕЗ ENUM ТОЖЕ ЛОМАЕТСЯ НЕ В ЛОБ. УЯЗВИМЫ САМИ СРЕДСТВА СВЯЗИ

ВЗЛОМ WEB-MONEY — НЕ МИФ, А СУРОВАЯ РЕАЛЬНОСТЬ



альтернативных браузеров типа Opera и FireFox выпущены плагины, они работают кое-как, и в реальности приходится использовать именно IE, количество дыр в котором достойно книги рекордов Гиннеса — создатели WebMoney сами подсаживают нас на дырявый браузер. Так что проблема коренится не в пользователях. Проблема в мозгах разработчиков (точнее, в их полном отсутствии) и в концепции всей системы. Проблема в принципиальной уязвимости протокола передачи денег и незащищенности Кеерега. Сколько лет уже существуют алгоритмы генерации «одноразовых» ключей, при котором воровать просто нечего и нечем? Но почему о них не знают разработчики платежной системы?

защищенность keeper light Если небезопасность классического Кеерега — общеизвестный факт, то Light считается достаточно защищенным. «В Keeper Classic файл с ключами можно по частям перетаскать, почту можно взломать и т.д. Ключи, хранящиеся на сменном носителе, троян может переписать на винчестер в момент, когда дискета или CD вставлены. То есть теоретически возможно добраться до денег, хотя при соблюдении всех мер предосторожности — крайне сложно. Но Light с неэкспортируемым сертификатом дает 100% гарантию безопасности», — взято с <http://owebmoney.ru/cafe/index.php?showtopic=108>.

Звучит заманчиво, но как обстоят дела на практике? Попробуем разобраться. Начнем с вопроса о том, как все-таки работает Кеерг Light. Очень просто. Секретный ключ теперь хранится не в KWM-файле, а в специальном сертификате, а все управление идет через web-интерфейс по специальным криптографическим протоколам.

Где браузер хранит сертификаты? Это зависит от браузера. Например, Mozilla — в каталоге «./mozilla/default/<blahblah/>/cert8.db», а IE, запущенный под управлением Windows XP Professional, использует довольно навороченную систему. Сертификаты с открытыми ключами хранятся в персональном (personal) хранилище, расположенном в каталоге Documents-n-Settings\<username>\Application-Data\Microsoft\SystemCertificates\My\Certificates. Эта информация открыта и доступна всем желающим. Сертификаты пользователя расположены в его профиле. Закрытые ключи хранятся в каталоге Documents-n-Settings\<username>\Application Data\Microsoft\Crypto\RSA. Все файлы, расположенные здесь, автоматически шифруются случайным симметричным ключом — основным ключом пользователя (user's master key) длиной в 64 символа. Основной ключ генерируется по алгоритму Triple DES на основе пользовательского пароля, с которым он входит в систему.

Что значит вся эта теоретическая бодяга в практическом плане? Стащить сертификат с закрытым ключом из-под Windows XP не удастся! То

есть удастся, но толку от этого будет ноль, поскольку на чужом компьютере он просто не заработает (на то он и закрытый сертификат). Правда, его можно экспортировать даже не обладая никакими особенными привилегиями. Распотроши программу Менеджера Сертификатов, если не знаешь как. Собственно говоря, для переноса сертификатов с компьютера на компьютер Keeper Light использует экспортируемый сертификат, который хранится в файлах с расширением .pfx, их можно встретить как на внешних носителях, так и на жестких дисках.

Здесь есть одно «но». Экспортируемый сертификат закрыт паролем, который был назначен пользователем, и чтобы импортировать его в свою систему, необходимо либо закинуть клавиатурный шпион, либо попробовать вскрыть пароль методом перебора. Первое слишком заметно, второе — долго, поэтому кража сертификатов не получила большого распространения.

Означает ли это, что Keeper Light защищен? Нет и еще раз нет. Если Keeper Classic можно защитить хотя бы теоретически (установить драйвер, обеспечивающий прямой клавиатурный ввод, отсекающий эмуляторы и следящий за целостностью Кеерера и самого себя), то Keeper Light работает через браузер, «целостность» которого невозможно контролировать в принципе!

Первое, что приходит на ум, — это упомянутая эмуляция. Говоришь «start <https://light.webmoney.ru>», тем или иным способом прячешь окно браузера (достаточно получить его дескриптор — и уже рисуешь поверх него что попало) и эмулируешь последовательность нажатия клавиш для пополнения электронного кошелька. Действует железно и неотвратимо. Единственный минус кроется в том, что каждый тип браузера (и, возможно, версия) требует особого подхода, но можно остановиться только на IE 5/6, как на самом популярном.

С остальными браузерами еще проще. Берешь исходники Firefox и создаешь хакерский мини-браузер на их основе, который ничего не выводит на экран, но с кошельками работает только так. Правда, среди пользователей WebMoney не так уж много поклонников Firefox, но это все же лучше, чем совсем ничего :). Кстати, пусть приверженцы IE не чувствуют себя в безопасности: исходные тексты W2K были украдены уже давно, и создать свой клон IE на их основе вполне реально, не говоря уже о том, что IE — это просто набор DCOM-объектов, собрать свой браузер на их основе сможет даже начинающий.

А что если импортировать сертификат перед каждым открытием кошелька, а затем удалять его из хранилища? Действительно, это до некоторой степени увеличит защищенность. Однако хакерская программа может либо дожидаться появления окна «WebMoney Кеерер :: Light Edition» (сигнализирует о том, что пользователь вошел в систему), либо шпионить за клавишами, передавая секретный пароль вместе с сертификатом по Сети. Так что электронные деньги все равно остаются в щекотливой ситуации...

надежность авторизации по сотовому телефону Последним пиком моды стала система авторизации с помощью сотового телефона. При регистрации в службе ENUM (<http://enum.ru>) на твой мобильник устанавливается специальное Java-приложение (мидлет). Приложение называет себя Enum Client, принимает пятизначные числа (например 09652) и генерирует на их основе ответ, причем алгоритм генерации уникален для каждого пользователя. Если у владельца кошелька нет сотового телефона, подойдет Pocket PC или любое другое устройство с поддержкой Java.

Служба ENUM позволяет совершать покупки через сервис Merchant (<https://merchant.webmoney.ru>), вообще не прибегая к Кеереру (ни к классическому, ни к облегченному). Считается, что взломать электронный кошелек и похитить наличность в этом случае уже не удастся. «Мошенники и вирусописатели используют интернет для кражи ценной информации с наших компьютеров. Но какую бы защиту мы ни изобрели — файрволы, антивирусы, антикейлогеры, антитрояны, сертификаты — всегда есть теоретическая вероятность ее обхода и кражи паролей с компьютера, потому что и хакеры, и защитные инструменты используют ОДИН И ТОТ ЖЕ канал — интернет. И проблема интернета состоит в том, что не существует альтернативного канала хранения-передачи информации. ENUM решает эту проблему, предоставляя нам тот самый другой канал. Ха-

кер может влезть на компьютер, «подсадить» троянский вирус, но он не сможет влезть в мобильный телефон. Угадать же, по какому уникальному для каждого пользователя алгоритму Enum Client из одного числа получает другое, тоже нельзя», — взято с <http://owebmoney.ru/enum.shtml>.

Действительно ли это так? Как говорится, если нельзя, но очень хочется, то все-таки можно :). Дополнительный «канал связи» и в самом деле многократно усиливает безопасность, но говорить о принципиальной невозможности взлома преждевременно. Начнем с того, что алгоритм генерации номеров для всех пользователей все-таки един (дизассемблируй мидлет, если не веришь), но ключ генерации разный и подобрать его вполне можно. Достаточно перехватить единственный отклик для данной комбинации цифр. Восстановление ключа не займет много времени, и оно вполне по силам троянской программе.

К тому же сотовые телефоны содержат кучу дыр, ИК-протоколы и Голубой Зуб буквально кишат ими. Если жертва имеет сотовый телефон или КПК, то, возможно, пользуется и адаптером Голубого Зуба или ИК, который держит постоянно включенным. Злоумышленник может передавать телефону любые AT-команды, выполнять мидлеты или считывать их содержимое. Можно написать вирус, похищающий электронные кошельки и передающий их через сотовый телефон. В обход всех брандмауэров! Вот тебе и дополнительный канал связи...

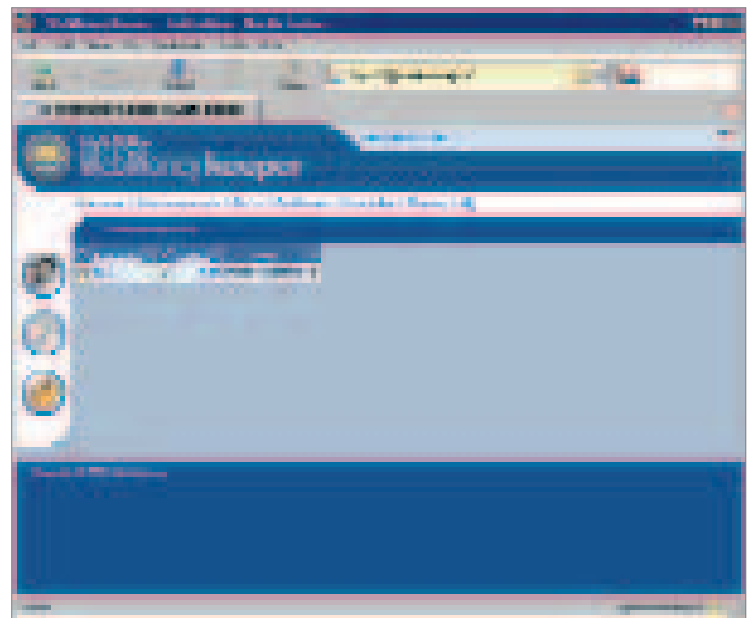
Впрочем, если посмотреть правде в глаза, необходимо признать, что хакнуть ENUM очень сложно. Но это не значит, что можно заводить электронный кошелек и смело класть на него \$100 000. Тогда точно взломают!

кровавая война продолжается Взлом WebMoney — это не миф, а суровая реальность. Обезопасить себя на 100% нельзя, даже если ты эксперт по безопасности. Всегда существует риск подхватить вирус через еще не известную дыру в операционной системе или браузере. Если от потери оперативных данных на винчестере спасает резервирование, от раскрытия конфиденциальных данных — физическое отключение интранета от Сети, то от кражи электронных денег не спасает ничто!

ЕСЛИ УВЕЛИ ДЕНЬГИ, ОСТАЕТСЯ ЕЩЕ ОДИН ШАНС — ОБРАТИТЬСЯ К АДМИНИСТРАТОРУ АРБИТРАЖНОГО СЕРВИСА

ПОДТВЕРЖДЕНИЕ АВТОРИЗАЦИИ ПО E-MAIL ЗАЩИЩАЕТ, НО ДОСТУП К ПОЧТЕ ТОЖЕ МОЖНО ДОБЫТЬ

Keeper Light — веб-интерфейс для работы с кошельком через любой браузер



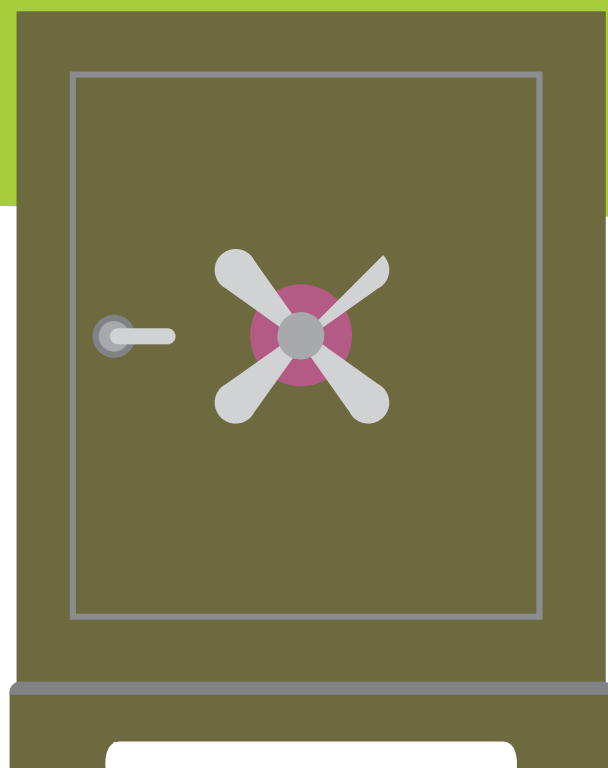
чей safe лучше?

РЕЙТИНГ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

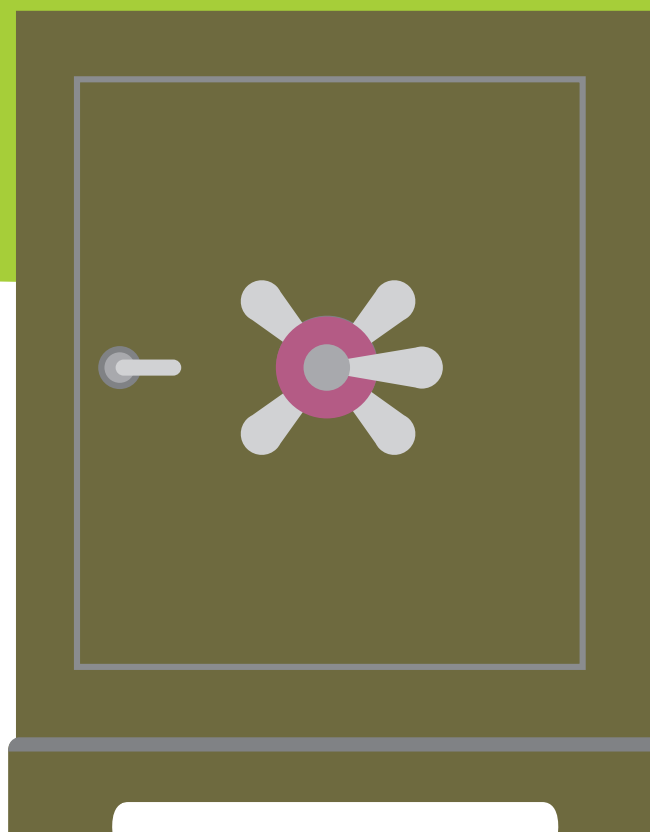
ВОПРОС БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ДЕНЕГ ВСЕГДА БЫЛ И ОСТАЕТСЯ ОДНИМ ИЗ ОСНОВНЫХ ФАКТОРОВ, КОТОРЫЕ СДЕРЖИВАЮТ РАЗВИТИЕ ЭТОГО РЫНКА. В ЭТОМ РЕЙТИНГЕ МЫ ПРОТЕСТИРУЕМ ЧЕТЫРЕ ОСНОВНЫЕ РОССИЙСКИЕ ПЛАТЕЖНЫЕ СИСТЕМЫ, ЧТОБЫ ОПРЕДЕЛИТЬ, КАКАЯ ИЗ НИХ САМАЯ НАДЕЖНАЯ | ДМИТРИЙ ДЕНЕЖКО АКА DENGA (DENEZKO@DMITRY.RU)

Для начала немного расскажу об использованной методике, простой до нельзя: оценим все четыре системы (Webmoney, «Яндекс.Деньги», CyberPlat и E-Port) по одним и тем же критериям, каждому из которых соответствует определенная шкала оценок. Сами же системы на выходе будут ранжироваться по совокупному количеству баллов, набранных в ходе каждого испытания.

Будем оценивать по многоуровневой системе, которая включает вложенные параметры. Разумеется, все эти критерии относятся к сфере информационной безопасности, так как мы составляем именно рейтинг безопасности электронных платежных систем. У нас есть два основных критерия: техническое обеспечение информационной безопасности платежей и организационно-правовое обеспечение. Под вторым мы подразумеваем в первую очередь уязвимости платежной системы мошенничеству, фишингу и т.д. Каждый из двух этих параметров будем оценивать по трехбалльной системе. Шкала оценок именно такая, так как нынешнее развитие электронных платежных систем в нашей стране находится на таком уровне, что большинство их параметров можно описать лишь словами «да» или «нет». Соответственно, если система электронных платежей максимально соответствует какому-либо параметру, она получает высший бал (3), если совсем не соответствует — минимальный (0). Если в системе

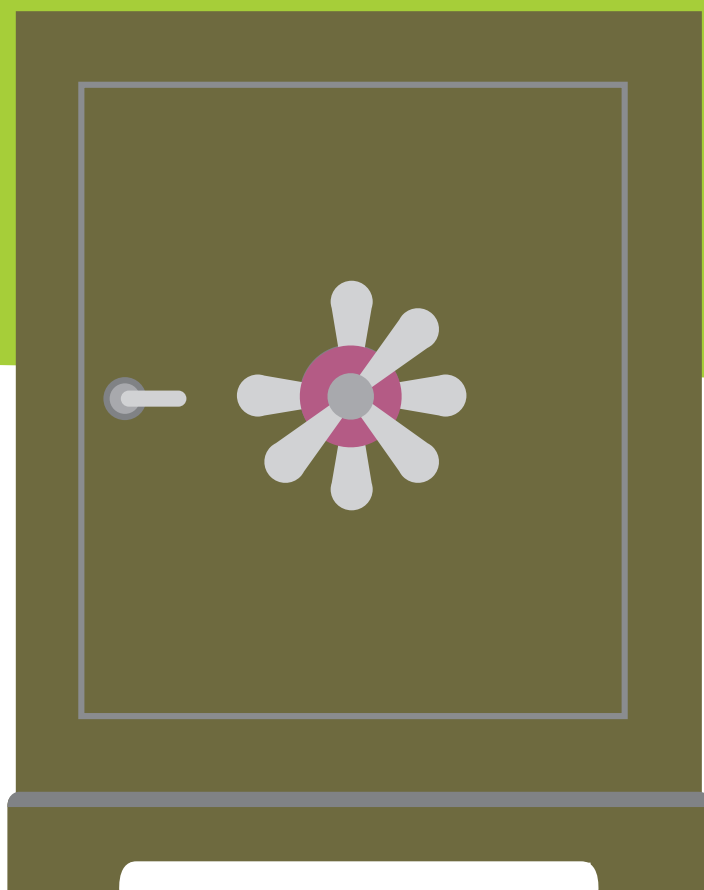


E-PORT
3,5 ОБОРОТА

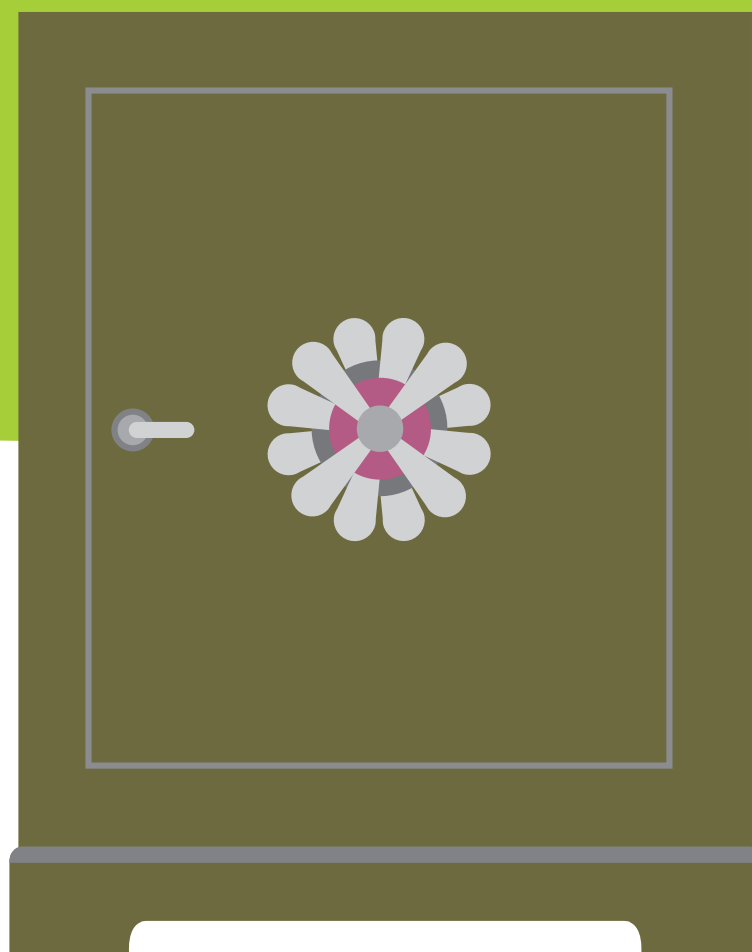


CYBERPLAT
5 ОБОРОТОВ

таблица оборота основных платежных систем									
СИСТЕМА/КРИТЕРИЙ	ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТРАНЗАКЦИЙ (БАЛЛЫ)				ОРГАНИЗАЦИОННО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ТРАНЗАКЦИЙ (БАЛЛЫ)				РЕЗУЛЬТАТ
	ШИФРОВАНИЕ	АУТЕНФИКАЦИЯ	ПРИМЕНЕНИЕ АППАРАТНЫХ КЛЮЧЕЙ ЗАЩИТЫ	ИТОГО	АНОНИМНОСТЬ	СИСТЕМА АТТЕСТАЦИИ	СИСТЕМА ЧЕРНЫХ СПИСКОВ	ИТОГО	
Webmoney	3	3	1,5	7,5	1,5	1,5	1,5	4,5	12
«Яндекс.Деньги»	3	3	0	6	1	0	0	1	7
Cyberplat	2	0	0	2	3	0	0	3	5
E-Port	1,5	1	0	2,5	1	0	0	1	3,5



«ЯНДЕКС.ДЕНЬГИ»
7 ОБОРОТОВ



WEBMONEY
12 ОБОРОТОВ

данного критерия в его явном виде нет, но если присутствуют какие-то сервисы или возможности, связанные с отсутствующим, присуждаем промежуточный бал — единицу или двойку. Какая именно из этих двух оценок будет выбрана, зависит от того, насколько конкретный дополнительный параметр связан с «исходным» критерием.

Оценивая системы электронных платежей, не забудем о том, что при разных условиях значения одного и того же параметра не одинаковы. Например, несколько сервисов, которые солидно повышают уровень защиты, могут быть реализованы пользователем только добровольно, дополнительно — ценно само наличие этих сервисов в системе. Человеческий фактор никто не отменял и никогда не отменит, поэтому мы будем учитывать, что сервис может быть как реализован, так и не реализован. Получается, что мы обязаны вводить весовой коэффициент для каждого параметра: для обязательных сервисов выставляем «1», а для сервисов, которыми пользуются только добровольно, — «0,5». Приступим.

техническое обеспечение безопасности транзакций

Это первый из наших критериев — набор параметров, обеспечивающий, как ясно из его названия, техническую сторону защиты информации. В этот параметр включены: криптографические методы шифрования, аутентификация и доступ при помощи специального аппаратного обеспечения (в самом примитивном случае — с помощью USB-ключей). Начинаем анализ.

Ни для кого не секрет, что основным критерием защиты информации в техническом плане является, конечно, шифрование данных, а конкретнее — криптографические алгоритмы, с помощью которых они реализованы. Известно также, что чем больше длина ключа, тем труднее расшифровать его и, соответственно, получить доступ к конфиденциальной информации. Три из «испытываемых» систем используют широко известный и широко уважаемый алгоритм RSA: Webmoney, «Яндекс.Деньги», Cyberplat. В E-Port применяется шифрование через SSL-протокол версии 3.0. Фактически шифрование реализовано с помощью SSL-ключей, которые уникальны и генерируются во время сессии, поэтому и названы сеансовыми ключами. Длина SSL-ключа в системе E-Port варьируется в пределах от 40 до 128-ми бит, что, по оценкам экспертов, вполне достаточно для приемлемого уровня безопасности транзакций.

В системах Webmoney, «Яндекс.Деньги» и Cyberplat, как я уже упоминал, для шифрования данных используется криптографический алгоритм RSA. При этом системы используют ключи разной длины. К примеру, в Webmoney и «Яндекс.Деньги» применяется ключ длиной 1024 бита (очень высокий показатель, взломать такой ключ методом простого перебора практически невозможно), а в Cyberplat используется ключ в два раза короче — 512 бит. Соответственно, для первых двух систем по этому критерию получаем максимальный балл — 3. Cyberplat, из-за того что применяет ключ шифрования меньшей длины, получает два балла. Остается только оценить по этому параметру E-Port.

Несмотря на использование в ней SSL-протокола и даже на длину ключа до 128-ми бит, в E-Port есть некоторая потенциальная уязвимость: многие старые версии браузеров поддерживают шифрование с ключами меньшей длины, поэтому существует возможность взломать полученные данные; соответственно, для тех, кто использует браузер как клиент для платежной системы, обязательно работать с его последней версией (конечно, это не всегда удобно и возможно). Однако в графе «шифрование» мы можем выставить для E-Port 1,7 балла, система зас-

ПРАКТИЧЕСКИ ВО ВСЕХ РАССМАТРИВАЕМЫХ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ ДЛЯ ШИФРОВАНИЯ ПРИМЕНЯЕТСЯ КРИПТОГРАФИЧЕСКИЙ АЛИГОРИТМ RSA

ДЛИНА SSL-КЛЮЧА В СИСТЕМЕ E-PORT ВАРЬИРУЕТСЯ В ПРЕДЕЛАХ ОТ 40 ДО 128 БИТ

В WEBMONEY ДЛЯ БОРЬБЫ С МОШЕННИЧЕСТВОМ РАБОТАНА СПЕЦИАЛЬНАЯ ИЕРАРХИЧЕСКАЯ СИСТЕМА АТТЕСТАЦИИ

лужила такую оценку благодаря применению прогрессивного протокола PGP для шифрования сообщений электронной почты.

Следующий параметр в «техническом обеспечении информационной безопасности транзакций» — «аутентификация», то есть совокупность решений, которые нужны пользователю для доступа к его собственной персональной информации. Здесь все довольно просто. В системах Webmoney и «Яндекс.Деньги» для доступа используются два критерия, в то время как в Cyberplat и E-Port — только один. В Webmoney для доступа в систему и проведения платежей необходимо вводить пароль и специальный ключ. Подобно работает и «Яндекс.Деньги»: требуется пароль и специальная программа-кошелек. Во всех остальных системах доступ осуществляется по паролю.

Однако в системе E-Port для работы по SSL-протоколу web-сервер потенциального клиента (и любого другого участника системы) должен иметь специальный цифровой сертификат, который получен от одной из уполномоченных компаний. Этот сертификат используется для аутентификации web-сервера клиента. Кстати, механизм защиты сертификата, который используется в E-Port, сертифицирован компанией RSA Security. Соответственно, Webmoney и «Яндекс.Деньги» получают здесь по троечке, Cyberplat — 0 баллов, E-Port — один.

Третий и последний параметр в нашем критерии — доступ к системе с помощью специального аппаратного обеспечения, например USB-ключей. Здесь еще проще, чем с предыдущими параметрами. Подобную дополнительную опцию из всех систем имеет лишь Webmoney, остальные не предоставляют такой возможности. Однако,

почему они не кинут?

ДЕЙСТВИТЕЛЬНО, ТВОИ ЧЕСТНО ЗАРАБОТАННЫЕ ДЕНЬГИ, ПУСТЬ ДАЖЕ ЭЛЕКТРОННЫЕ, МОГУТ ПРОПАСТЬ НЕ ТОЛЬКО ИЗ-ЗА ВСЯКИХ МОШЕННИКОВ. ВИНОВАТЫМИ МОГУТ ОКАЗАТЬСЯ И ВИРУСЫ, И ФИШИНГ — МНОГО РАЗНОГО ЗЛА СУЩЕСТВУЕТ. ЧТО ЖЕ МЕШАЕТ САМОМУ ОПЕРАТОРУ ЭЛЕКТРОННОЙ ПЛАТЕЖНОЙ СИСТЕМЫ «КИНУТЬ» ТЕБЯ? НАБРАЛ ПОЛЬЗОВАТЕЛЕЙ (ДЛЯ ОБОГАЩЕНИЯ ОДНОГО ЧЕЛОВЕКА, ВЛАДЕЛЬЦА ПЛАТЕЖНОЙ СИСТЕМЫ, МНОГО ЛЮДЕЙ НЕ НАДО), НЕ МНОГО ПОТЯНУЛ С ТРАНЗАКЦИЯМИ (ПОКА НЕ ЗАПАХЛО ЖАРеным) И СБЕЖАЛ КУДА ПОДАЛЬШЕ (ПОКА ДОБЛЕСТНОЕ УПРАВЛЕНИЕ «К» НЕ ПОЙМАЕТ). КАРАУЛ! КИНУТЬ ТЕБЯ ОЧЕНЬ ПРОСТО! НО НЕ СОВСЕМ ПРОСТО И ДАЖЕ ОЧЕНЬ СЛОЖНО. ВО-ПЕРВЫХ, ВРЕМЯ АБСОЛЮТНОЙ ДИКОСТИ БИЗНЕСА В РОССИИ УЖЕ ПРОШЛО, СЕГОДНЯ ВСЕ СКОЛЬКО-НИБУДЬ ЗНАЧИМЫЕ ИГРОКИ РЫНКА ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ ИМЕЮТ ДОСТАТОЧНО ВНЯТНЫЙ ЮРИДИЧЕСКИЙ СТАТУС. КРОМЕ ТОГО, ЗА СПИНОЙ E-MONEY-СИСТЕМ ОБЫЧНО СТОЯТ РЕАЛЬНЫЕ ФИНАНСОВЫЕ СТРУКТУРЫ, КОТОРЫЕ И ВЫСТУПАЮТ ГАРАНТОМ ОБЕСПЕЧЕНИЯ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ. НЕ ЗАБУДЬ ТАКЖЕ И ТО, ЧТО ОБМАН НЕВЫГОДЕН ДЛЯ СЕРЬЕЗНОГО ИГРОКА, ЕГО ПРИБЫЛЬ СТРОИТСЯ ПО ПРИНЦИПУ ПИРАМИДЫ, ТАК КАК ОБЫЧНО ОПЕРАТОР ЭЛЕКТРОННОЙ ПЛАТЕЖНОЙ СИСТЕМЫ (ЧАЩЕ ВСЕГО ОН ЖЕ — ЕЕ ВЛАДЕЛЕЦ) ПОЛУЧАЕТ ПРИБЫЛЬ С КОМИССИЕЙ КАЖДОЙ ТРАНЗАКЦИИ. ТАК ЧТО РУБИТЬ СУК, НА КОТОРОМ СИДИШЬ, НАВЕРНОЕ, НЕ ЗАХОЧЕТ НИКТО.

ЛЮБОЙ УЧАСТНИК СИСТЕМЫ, КОТОРЫЙ СЧИТАЕТ, ЧТО ЕГО ОБМАНУЛИ ИЛИ ЧТО С НИМ ПОСТУПИЛИ НЕЧЕСТНО, МОЖЕТ ОСТАВИТЬ ЖАЛОБУ ИЛИ ПРЕТЕНЗИЮ НА ДРУГОГО УЧАСТНИКА СИСТЕМЫ

Кроме того, различные аттестаты предоставляют различные уровни сервиса со стороны системы, и это значительно стимулирует участников системы быть максимально открытыми. Тем не менее, система аттестации является добровольной — вот и лазейка для мошенников. Подобное решение имеется только в WebMoney, поэтому по параметру «анонимности», с учетом весового коэффициента, выставим ей 1,5 балла.

Я не случайно упомянул о построении некой социальной сети пользователей электронных платежных систем. Это действительно очень полезное и необходимое действие для выстраивания прозрачного рынка электронных платежей. Третий параметр, который мы рассмотрим для оценки «организационно-правового обеспечения безопасности транзакций», — система «черных списков».

Увы, это решение реализовано в одной-единственной рассмотренной платежной системе — Webmoney, которая вообще уделяет много внимания необходимости построения социальной сети пользователей. Система аттестации, о которой мы говорили, и система «черных списков» (англ. blacklist) весьма эффективно решают эту задачу. Суть blacklist состоит в том, что любой участник системы, который считает, что его обманули или что с ним поступили нечестно, может оставить жалобу или претензию на другого участника системы. Очень важно то, что подобные жалобы/претензии доступны для просмотра всем участникам системы, которые пытаются провести транзакцию с пользователем, на которого выставлена подобная информация. Удобно! Плюс наличие blacklist повышает доверие между конкретными участниками системы и, соответственно, позволяет эффективно выстраивать упоминутую социальную сеть.

Дополнительно в Webmoney реализована так называемая система арбитража. Если складывается неоднозначная ситуация, любой пользователь системы может обратиться в «арбитражный суд» Webmoney и, описав возникшие спорные моменты, после детального анализа получить определенное решение по данному вопросу. Итого, по совокупности данных параметров система Webmoney завоевала максимальный балл (с учетом весового коэффициента — 1,5), а другие участники рейтинга, из-за несоответствия данным параметрам, получают минимальную оценку.

Смотри на www...

ФИШИНГ — ЭЛЕМЕНТАРНЕЙШИЙ (НО ОЧЕНЬ ЛЮБИМЫЙ МОШЕННИКАМИ) СПОСОБ ХИЩЕНИЯ ЧУЖИХ ЭЛЕКТРОННЫХ ДЕНЕГ. ЕСЛИ ГОВОРИТЬ ТОЧНЕЕ, ОН ПРЕДСТАВЛЯЕТ СОБОЙ ИСПОЛЬЗОВАНИЕ ПОДСТАВНЫХ САЙТОВ. СХЕМА ФИШИНГА ПРОСТА ДО БЕЗОБРАЗИЯ. У ТЕБЯ ЕСТЬ ЛЮБИМЫЙ ОБМЕННИК, КОТОРЫМ ТЫ ПОЛЬЗУЕШЬСЯ ПОСТОЯННО. ОХОЧИЙ ДО ТВОИХ ДЕНЕГ ЧЕЛОВЕК ВЫЯСНЯЕТ ТВОИ ПРЕДПОЧТЕНИЯ, СОЗДАЕТ СПЕЦИАЛЬНЫЙ САЙТ — ТОЧНУЮ КОПИЮ ТОГО САМОГО «ТВОЕГО» ОБМЕННИКА. ВОТ ТЫ ЗАШЕЛ НА «ПОДДЕЛКУ», НИЧЕГО НЕ ПОДОЗРЕВАЕШЬ, ВВОДИШЬ СВОЙ ПАРОЛЬ И ЖДЕШЬ РЕЗУЛЬТАТОВ ТРАНЗАКЦИИ, А ТЕМ ВРЕМЕНЕМ ВСЕ ТВОИ РЕКВИЗИТЫ УЖЕ ПРИОБРЕЛИ НОГИ И УШЛИ К МОШЕННИКУ. ТАК ЧТО ВСЕГДА ВНИМАТЕЛЬНО СМОТРИ НА АДРЕС САЙТА. ХОТЯ И ЭТО ПОДДЕЛАТЬ НЕТРУДНО...

червь в кошельке

В ЭТОЙ СТАТЬЕ МЫ РАССМОТРЕЛИ ВСЕ ФАКТОРЫ, СВЯЗАННЫЕ С ПОСТРОЕНИЕМ СОЦИАЛЬНОЙ СЕТИ УЧАСТНИКОВ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ. ЧЕРНЫЕ СПИСКИ И Т.П., КОНЕЧНО, ПОМОГАЮТ ЧЕСТНЫМ ГРАЖДАНАМ, НО ЭТИ МЕРЫ ДОПОЛНИТЕЛЬНЫЕ И ОНИ НЕ СПАСУТ ОТ «ПРЯМЫХ» МОШЕННИКОВ — ТЕХ, КТО ИСПОЛЬЗУЕТ ДЫРЫ В ПРОГРАММНОМ ОБЕСПЕЧЕНИИ, ЧТОБЫ ЗАВЛАДЕТЬ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ. ТРОПИНОК, ПО КОТОРЫМ ЗЛОДЕИ ОБХОДЯТ ЗАЩИТУ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ, ВЕЛИКОЕ МНОЖЕСТВО, НО, НАВЕРНОЕ, САМАЯ ПОПУЛЯРНАЯ ИЗ НИХ — ИСПОЛЬЗОВАНИЕ ТРОЯНСКИХ ЧЕРВЕЙ. ДЕЙСТВИТЕЛЬНО, ЛЮДИ ВСЕГДА БЫЛИ ЖАДНЫ ДО ЧУЖОГО, А УЖ КОГДА ИМ ГОВОРЯТ «ВНИМАНИЕ! ТУТ ЗАРЫТЫ ДЕНЬГИ!»... САМ ПОНИМАЕШЬ. ТАК ВОТ, ПЛОХИЕ ХАКЕРЫ ВЗЯЛИ И НАПИСАЛИ СПЕЦИАЛЬНЫЕ ВИРУСЫ — ИСКЛЮЧИТЕЛЬНО ДЛЯ КРАЖИ ЭЛЕКТРОННЫХ ДЕНЕГ.

К ПРИМЕРУ, ОТНОСИТЕЛЬНО НЕДАВНО БЫЛ ЗАРЕГИСТРИРОВАН ТРОЯНЕЦ BANCOS.FC (ДОСТОЙНОЕ НАЗВАНИЕ, ОНО ГОВОРИТ САМО ЗА СЕБЯ). ЭТОТ ТРОЯНСКИЙ ЧЕРВЬ ПРЕДНАЗНАЧЕН СПЕЦИАЛЬНО ДЛЯ КРАЖИ ДАННЫХ, КОТОРЫЕ ОТНОСЯТСЯ К БАНКОВСКИМ СЧЕТАМ, И ПОСЛЕДУЮЩЕЙ ОТПРАВКИ ЭТИХ ДАННЫХ НА СПЕЦИАЛЬНЫЙ АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ. МЕХАНИЗМ ЕГО РАБОТЫ ДОСТАТОЧНО ПРОСТ. ПОЛЬЗОВАТЕЛЬ ЗАПУСКАЕТ ФАЙЛ, СОДЕРЖАЩИЙ BANCOS.FC, И ВИРУС УСТАНОВЛИВАЕТСЯ В СИСТЕМУ, СОЗДАВАЯ СВОЮ КОПИЮ ПОД ИМЕНЕМ FTREX.EXE, А ТАКЖЕ БИБЛИОТЕКУ FTREX.DLL. ПОСЛЕДНЯЯ СОДЕРЖИТ ИНТЕРНЕТ-АДРЕСА РАЗЛИЧНЫХ ФИНАНСОВЫХ УЧРЕЖДЕНИЙ ПО ВСЕМУ МИРУ (КСТАТИ, БОЛЬШЕ ВСЕГО ВНИМАНИЯ ТАМ УДЕЛЕНО ИСПАНОГОВОРЯЩИМ СТРАНАМ). ТАК ВОТ FTREX.DLL ЗАПУСКАЕТСЯ КАЖДЫЙ РАЗ, КОГДА ПОЛЬЗОВАТЕЛЬ ЖДЕТ ИСПОЛНЕНИЯ INTERNET EXPLORER, ТО ЕСТЬ ПРАКТИЧЕСКИ ВСЕГДА, КОГДА ТРЕБУЕТСЯ ПРОВЕСТИ КАКУЮ-ЛИБО ТРАНЗАКЦИЮ. ПРИ СОЕДИНЕНИИ ТРОЯНСКИЙ ЧЕРВЬ ПРОВЕРЯЕТ КАЖДЫЙ ВВОДИМЫЙ URL, ЧТОБЫ ОПРЕДЕЛИТЬ, СОВПАДАЕТ ЛИ ОН С КАКИМ-ЛИБО ИЗ ЕГО СПИСКА. URL И ВСЕ НЕОБХОДИМЫЕ ДАННЫЕ, ТАКИЕ КАК НОМЕР СЧЕТА, НОМЕР КРЕДИТНОЙ КАРТЫ, ПАРОЛЬ И Т.Д., СОХРАНЯЮТСЯ, ЗАТЕМ ОТПРАВЛЯЮТСЯ НА ПОЧТОВЫЙ ЯЩИК ХАКЕРА.

ДЛЯ ПРЕДОТВРАЩЕНИЯ МОШЕННИЧЕСТВА НЕОБХОДИМО ВЫСТРАИВАТЬ СОЦИАЛЬНУЮ СЕТЬ УЧАСТНИКОВ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ

Осталось только свести все параметры в единую таблицу и определить лидера нашего рейтинга — по сумме набранных баллов.

подведем итоги Собственно, после оценки двух критериев, как мы договаривались в самом начале, можно подвести итоги. По сумме рассмотренных параметров самой безопасной оказалась Webmoney. Действительно, если пользователь задействует все предоставленные ей сервисы обеспечения безопасности, он может остаться фактически неуязвимым для мошенников. Второе место заняла система «Яндекс.Деньги», третье — Cyberplat (эта система идеально подойдет юридическим лицам из-за значительной юридической прозрачности платежей), а последнее место присуждено системе E-Port. Однако не забудем, что при составлении рейтинга учитывались далеко не все возможные параметры, а только те, оценить которые можно довольно легко и наглядно. Так что при более глубоком подходе результаты, скорее всего, оказались бы распределены по участникам рейтинга более равномерно.

Кроме того, выбор электронной платежной системы осуществляется вовсе не по одному параметру безопасности, пусть даже он один из самых важных. Системы электронных платежей также отличаются наличием сервисов, удобством использования — есть множество других факторов. Окончательное решение о выборе системы электронных платежей принимай оценив максимальное количество факторов, а какие из них важнее всего — решать тебе.

ЧИТАЙ В СЛЕДУЮЩЕМ НОМЕРЕ СПЕЦА:

ФАЙЛОВЫЕ ХРАНИЛИЩА ОНЛАЙН
СОВРЕМЕННЫЕ ВИНЧЕСТЕРЫ
КАК ХРАНИТЬ ДАННЫЕ В ДОМАШНИХ УСЛОВИЯХ
МЕГАТЕСТ АРХИВАТОРОВ
ЗАЧЕМ НУЖЕН ВАСКУР?
ВАСКУР ДЛЯ АДМИНА
РАСПРЕДЕЛЕННЫЕ ХРАНИЛИЩА В LAN
ПОЛНОЕ ВОССТАНОВЛЕНИЕ
ШИФРОВАННЫЕ ДИСКИ
ВЗЛОМ ЗАЩИЩЕННЫХ ФАЙЛОВ

А также: резервные носители, backup
в *nix и множество других способов
сохранить ценную информацию!

НАДЕЖНОЕ
ХРАНЕНИЕ
ДАННЫХ
И ВАСКУР





платить предохраняясь

ОБЕСПЕЧЕНИЕ НАДЕЖНОГО ПРОЦЕССИНГА В ЭЛЕКТРОННЫХ МАГАЗИНАХ

НА ЗАПАДЕ ПРАКТИЧЕСКИ ВСЕ ИНТЕРНЕТ-МАГАЗИНЫ НЕ РАБОТАЮТ С НАЛИЧНЫМИ ДЕНЬГАМИ — ПОКУПАТЕЛЬ, ЗАКАЗЫВАЯ ТОВАР, ОПЛАЧИВАЕТ ЕГО НА САЙТЕ МАГАЗИНА ПЛАСТИКОВОЙ КАРТОЧКОЙ, ВИРТУАЛЬНОЙ КРЕДИТКОЙ ИЛИ ЧЕРЕЗ КАКУЮ-ЛИБО СИСТЕМУ ЭЛЕКТРОННЫХ ДЕНЕГ | ПЕТЯ МОКИН (TOFFLER@MAIL.RU)

НЕСМОТЯ НА ДОВОЛЬНО ПРОСТОЙ ИНТЕРФЕЙС, «ЯН-ДЕКС.ДЕНЬГИ» МАЛО УСТУПАЕТ WEB-MONEY

В России до сих пор одна из основных форм оплаты — «наличными курьеру». Покупатель заказывает товар на сайте магазина, а оплачивает его наличными в момент доставки курьером. Подобная форма более-менее устраивает и магазин, и покупателя. Магазины не нужно возиться с приемом безналичных платежей, при этом также снимается проблема charge back — отзывов платежей владельцами пластиковых карточек. Покупателю к тому же удобнее платить непосредственно в момент доставки товара — у нас не особенно приветствуется схема «сначала оплата, а потом товар», так как нередки случаи, когда после честной оплаты превращаешься в бедную Сольвейг, ожидающую своего Пера Гюнта, то есть вожделенный товар, который все не доставляют и не доставляют.

К сожалению, оплата наличными при доставке возможна далеко не во всех случаях. Существует масса товаров и услуг, приобретение которых никак не связано с появлением в твоём доме или офисе курьера, например регистрация программ через интернет, приобретение каких-то сервисов и т.д. Нет курьера — платить некому, точнее, придется платить прямо на сайте. Однако нас постоянно учат не светить номером своей карточки, не платить пластиком в интернете, иначе денежки уплывут черт знает куда, а от твоей карточки останется лишь номер.

Однако все страхи по поводу оплаты пластиком в интернете весьма преувеличены. Похоже на ситуацию с опасностью прогулок по улицам ночью: если в темное время суток ты забредешь в Гарлем будучи одетым в майку с надписью «Niggers must die», то... , а если ты будешь тихо и мирно гулять на охраняемой территории коттеджного поселка, то останешься цел и невредим. Так и в интернете: в одних райончиках (читай «сайтах») тебя действительно обчистят по полной программе, а в приличных местах опасность мизерная. Остается только отличать приличные районы от подозрительных кварталов. Какие же меры предосторожности ты должен предпринять, чтобы свести риск к минимуму и спокойно платить пластиком в интернете, не боясь повредить своему счету?

подозрительные райончики Можно долго не рассусоливать, ты сам знаешь эти подозрительные райончики, их видно за версту. Всевозможная порнуха, сайты с варезом и крэками... Словом, все, что выглядит как криминал, и является криминалом. Если на этих сайтах предлагают оплатить что-то пластиковой карточкой и ты слушаешься, продолжай, желаю тебе миллионов на счете, чтобы владельцам сайта было где разгуляться. Только не говори потом растерянно: «Вот черт, а с виду был такой приличный порнушный сайт».

WEBMONEY НЕ ЯВЛЯЕТСЯ ПЛАТЕЖНОЙ СИСТЕМОЙ ФОРМАЛЬНО, НО ПОЛНОСТЬЮ ЭКВИВАЛЕНТНА ЕЙ

«ДЕНЬГИ@MAIL.RU» ПОЯВИЛАСЬ СОВСЕМ НЕДАВНО И ПОКА МАЛО РАСПРОСТРАНЕНА

Впрочем, сами владельцы подобных сайтов, как правило, не воруют деньги со счетов, их обычный бизнес — это перепродажа полученных номеров пластиковых карт деятелям, которые как раз занимаются соответствующим воровством или покупкой товаров на украденные карточки с последующей реализацией товаров. Так сказать, легализация бизнеса.

Однако существует и целый ряд небольших онлайн-магазинов, предоставляющих вполне нормальные виды услуг, но использовать пластиковые карточки на этих сайтах все равно опасно. Не категорично, но справедливо к тем магазинчикам, которые самостоятельно принимают оплату (процессят твою кредитку), значит, хранят сведения о номерах карточек своих клиентов у себя на сайте. Будь внимателен к подобным ситуациям. Черт его знает, что за магазин, что за сайт, что за сотрудники и насколько это безопасно. Номер твоей кредитки могут продать негодьям. Или хакеры смогут поломать сайт магазина, чтобы увести всю клиентскую базу. Или кто-то из сотрудников магазина аккуратно перепишет эту базу на flash'ку и продаст за сумму, равную своей месячной зарплате, тем же негодьям.

приличные места Как же работают приличные интернет-магазины? Приличный российский интернет-магазин не станет заниматься приемом денег с пластика самостоятельно. Держать и охранять базу клиентов, обеспечивать безопасные транзакции и т.д. — это ненужные для солидных проектов дела. Процессингом пластиковых карточек занимаются специальные системы, им на откуп и отдаются подобные действия. Сапогами должен заниматься сапожник, печь пироги кондитер, а карточки должны процессить процессинго-

Юные кардеры и вполне предсказуемые последствия

НЕКАЯ ГРУППА, СОСТОЯЩАЯ ИЗ МОЛОДЫХ ЛЮДЕЙ 18-19-ТИ ЛЕТ, РЕШИЛА ЗАНЯТЬСЯ ВЫГОДНЫМ, КАК ИМ КАЗАЛОСЬ, БИЗНЕСОМ. ОДИН ИЗ ГРУППЫ ПОКУПАЛ В ИНТЕРНЕТЕ ИНФОРМАЦИЮ О ДЕЙСТВУЮЩИХ КРЕДИТНЫХ КАРТАХ (ТОЧНЕЕ, ОБ ИХ РЕКВИЗИТАХ) У ПОКА НЕ ОПРЕДЕЛЕННОГО ЛИЦА. ЕГО ПОДЕЛЬНИКИ ОТКРЫВАЛИ ТАК НАЗЫВАЕМЫЕ ВИРТУАЛЬНЫЕ ЭЛЕКТРОННЫЕ КАРТЫ (СЧЕТ, ПРИВЯЗАННЫЙ К КАРТЕ, КОТОРАЯ СУЩЕСТВУЕТ ТОЛЬКО В ВИДЕ РЕКВИЗИТОВ — НОМЕРА И ДИАПАЗОНА ДЕЙСТВИЯ), НА КОТОРЫЕ ПЕРЕВОДИЛИСЬ СРЕДСТВА С ВОРОВАННЫХ КРЕДИТОК. ТАКИМ ОБРАЗОМ, КАК СЧИТАЛИ МОЛОДЫЕ ЛЮДИ, ДЕНЬГИ «ОБЕЛЯЛИСЬ». НА ВИРТУАЛЬНЫЕ КАРТЫ ПРИОБРЕТАЛИСЬ РАЗЛИЧНЫЕ ТОВАРЫ. НАПРИМЕР, ТОЛЬКО В ИНТЕРНЕТ-МАГАЗИНЕ SOFTKEY МОШЕННИКИ ПРИОБРЕЛИ ТОВАРЫ НА 80 000 РУБЛЕЙ И ПЫТАЛИСЬ ПОЛУЧИТЬ ИХ НА СУММУ 60 000 РУБЛЕЙ.

КАК НИ СТРАННО, ПАРНЕЙ ПОЙМАЛИ ДОВОЛЬНО БЫСТРО. СНАЧАЛА БАНКИ ЗАМЕТИЛИ МОШЕННИЧЕСКИЕ ТРАНЗАКЦИИ С ВОРОВАННЫХ КРЕДИТОК, ЗАТЕМ ПРОСЛЕДИЛИ ВЛАДЕЛЬЦЕВ «ЧИСТЫХ» КАРТОЧЕК, ПОСЛЕ ЧЕГО ЗАСЕКЛИ ПОКУПКИ С УЖЕ ВИРТУАЛЬНЫХ «ЧИСТЫХ» ЭЛЕКТРОННЫХ КАРТ.

РАССМОТРЕНИЕ ПО ДАННОМУ УГОЛОВНОМУ ДЕЛУ УЖЕ ИДЕТ В ОСТАНКИНСКОМ СУДЕ МОСКВЫ. ДЕЙСТВИЯ МОЛОДЫХ ЛЮДЕЙ ПОПАДАЮТ ПОД ЧАСТЬ 4 СТАТЬИ 159 УК — МОШЕННИЧЕСТВО, СОВЕРШЕННОЕ ОРГАНИЗОВАННОЙ ГРУППОЙ. НАКАЗЫВАЕТСЯ ЛИШЕНИЕМ СВОБОДЫ НА СРОК ОТ ПЯТИ ДО ДЕСЯТИ ЛЕТ ПЛЮС ШТРАФОМ В РАЗМЕРЕ ДО ОДНОГО МИЛЛИОНА РУБЛЕЙ ИЛИ В РАЗМЕРЕ ЗАРАБОТНОЙ ПЛАТЫ, ИЛИ ИНОГО ДОХОДА ОСУЖДЕННОГО ЗА ПЕРИОД ДО ТРЕХ ЛЕТ ЛИБО БЕЗ ТАКОВОГО.

В РОССИИ ВСЕГО ТРИ ПРОЦЕССИНГОВЫХ ЦЕНТРА: ASSIST, CYBERPLAT И ПРОЦЕССИНГОВЫЙ ЦЕНТР «ИМПЭКСБАНКА»

вые центры — так гласит старая поговорка. В России три таких центра, и они общеизвестны: ASSIST, CyberPlat и процессинговый центр «ИМПЭКСБАНКА». Каждый из них подключен к своему эквайринг-банку. Эквайринг — это, так сказать, урегулирование платежных отношений между эмитентом карты (банком, выпускающим ее), ее держателем (это ты) и получателем платежа (магазином или сервисом). Эквайринг-банк регулирует эти взаимоотношения за соответствующую комиссию: в случае подтверждения платежа снимает деньги со счета плательщика и переводит их на счет магазина (сервиса).

Весь процесс платежа происходит следующим образом. Ты выбираешь товар или услугу, указываешь способ оплаты пластиковой карточкой, нажимаешь кнопку «Оплатить» или что-то подобное, после чего с сайта тебя перенаправляют на совершенно другой ресурс — страницу процессингового центра. Обрати внимание на то, что эта страница защищена со всех

сторон как различными сертификатами, так и другими средствами. Данные своей карты (неважно, кредитная карта, дебетовая или даже не пластиковая — электронная) ты будешь вводить именно там — на защищенном сайте, а вовсе не на сайте магазина.

Далее данные из процессингового центра поступают в эквайринг-банк. Тот отправляет данные в банк-эмитент (банк, выпустивший карту), эмитент подтверждает или не подтверждает и передает соответствующий ответ. По этой же цепочке данные возвращаются в магазин. Обычно процедура занимает несколько секунд, по истечении которых магазин имеет четкий ответ о том, подтвержден ли твой платеж банком. В любом случае процессинговому центру, вне зависимости от его выбора магазином, предоставляются весьма ограниченные данные о твоей карте. Например, сообщают последние четыре цифры, твое имя и название банка, воспользоваться которыми в неблагоприятных целях будет практически невозможно.

Такая система вполне безопасна для покупателя. Магазин не получает никаких вразумительных ценных данных о пользователе, процессинговый центр не сохраняет данные твоей карточки, а только передает их в банк-эмитент, который и так знает о тебе все, потому что открыл для тебя счет. Интернет-магазину также неинтересна подобная форма, потому что в этом случае сайт проекта не представляет интереса для взлома — какой смысл вскрывать его, если там ничего не хранится? Впрочем, солидный интернет-магазин также старается отслеживать и пресекать мошеннические операции.

реальный опыт: Softkey

XS: ПРИНЯТО ЛИ ОТСЛЕЖИВАТЬ ПЛАТЕЖИ В SOFTKEY?

ФЕЛИКС МУЧНИК, ДИРЕКТОР ОНЛАЙНОВОГО МАГАЗИНА SOFTKEY (www.softkey.ru; ЗАО «СОФТКЕЙ»): ДА, КОНЕЧНО. БОЛЕЕ ТОГО, У НАС ЕСТЬ СПЕЦИАЛЬНЫЙ ОТДЕЛ МОНИТОРИНГА, КОТОРЫЙ ОЦЕНИВАЕТ КАЖДЫЙ ПЛАТЕЖ ПО ЦЕЛОМУ РЯДУ И СОВОКУПНОСТИ ПАРАМЕТРОВ. СМОТРЯТ НА ВСЕ: СОСТАВ ЗАКАЗА, ВРЕМЯ СУТОК, В КОТОРОЕ ОФОРМЛЕН ЗАКАЗ, E-MAIL (МОШЕННИКИ ОБЫЧНО ИСПОЛЬЗУЮТ НИКИ, А НЕ ИМЯ, ИЛИ ЕГО ЧАСТЬ В ПОЧТОВОМ АДРЕСЕ) И МНОГОЕ-МНОГОЕ ДРУГОЕ, НЕ ГОВОРЯ УЖЕ О ТАКИХ БАНАЛЬНЫХ СЛУЧАЯХ, КАК ПОВТОРНЫЕ ПОПЫТКИ ОФОРМИТЬ ЗАКАЗ ПОД ДРУГИМ ИМЕНЕМ И ДРУГОЙ КАРТЕ ПОСЛЕ ТОГО, КАК ПЕРВЫЙ ЗАКАЗ БЫЛ ОТМЕНЕН ИЗ-ЗА ПОДОЗРЕНИЙ В МОШЕННИЧЕСТВЕ, ВОЗНИКШИХ У СОТРУДНИКОВ SOFTKEY. В СЛУЧАЕ ЕСЛИ У ОТДЕЛА МОНИТОРИНГА ВОЗНИКАЮТ ПОДОЗРЕНИЯ, ПРОВОДЯТСЯ РАЗЛИЧНЫЕ ДОПОЛНИТЕЛЬНЫЕ ПРОВЕРКИ: ТЕЛЕФОННАЯ АВТОРИЗАЦИЯ, ИЗУЧЕНИЕ РАЗЛИЧНЫХ ДОКУМЕНТОВ, ОТНОСЯЩИХСЯ К ДАННОМУ ЗАКАЗЧИКУ, И Т.Д.

XS: ПРИНОСЯТ ЛИ КАКУЮ-ЛИБО ПОЛЬЗУ ЭТИ ПРОВЕРКИ?

ФЕЛИКС МУЧНИК: ЗНАЧИТЕЛЬНУЮ ПОЛЬЗУ. НАПРИМЕР, В ЭТОМ ГОДУ С НАШЕЙ ПОМОЩЬЮ БЫЛА ОБНАРУЖЕНА ЦЕЛАЯ ГРУППА ЛИЦ, ЗАНИМАЮЩАЯСЯ МОШЕННИЧЕСТВОМ С ПЛАСТИКОВЫМИ КАРТАМИ В ИНТЕРНЕТЕ. И ПО ЭТОМУ ПОВОДУ БЫЛО ВОЗБУЖДЕНО УГОЛОВНОЕ ДЕЛО.

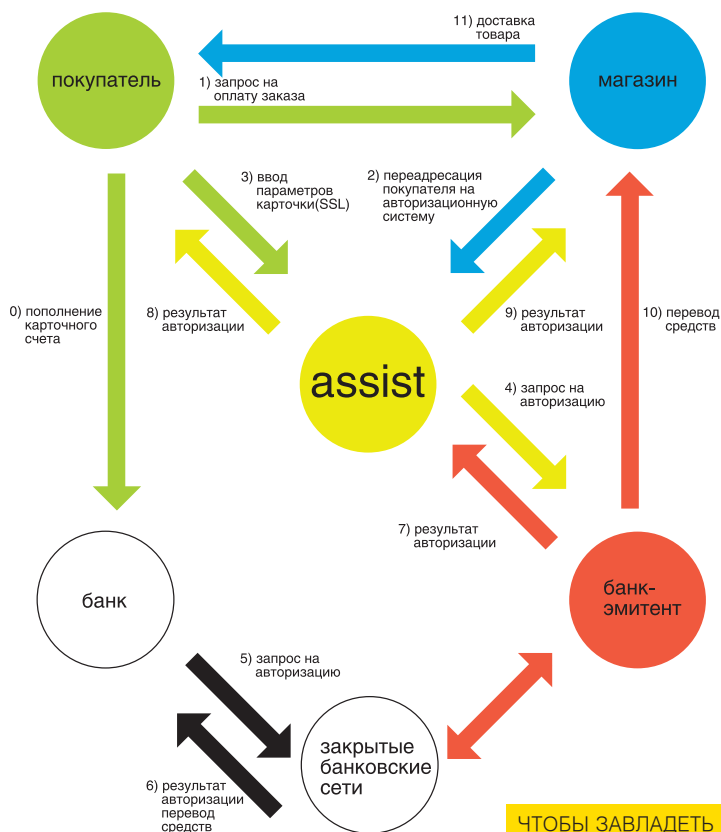
XS: КАКИЕ СОВЕТЫ ПО ПОВОДУ ЗАЩИТЫ ПЛАТЕЖЕЙ ВЫ МОГЛИ БЫ ДАТЬ ВЛАДЕЛЬЦАМ ДРУГИХ ОНЛАЙНОВЫХ МАГАЗИНОВ?

ФЕЛИКС МУЧНИК: ГЛАВНЫЙ СПОСОБ ЗАЩИТЫ — НЕ ЭКОНОМИТЬ НА БЕЗОПАСНОСТИ СИСТЕМЫ, НЕ ДЕЛАТЬ СИСТЕМЫ НА БЕСПЛАТНЫХ И ШИРОКО ИЗВЕСТНЫХ СКРИПТАХ (ИХ ОЧЕНЬ ЛЕГКО ВЗЛОМАТЬ), НЕ СТАВИТЬ СИСТЕМУ НА ВИРТУАЛЬНЫХ ХОСТИНГАХ, В ОБЯЗАТЕЛЬНОМ ПОРЯДКЕ УСТАНАВЛИВАТЬ АНТИВИРУСНУЮ И АНТИШПИОНСКУЮ ЗАЩИТУ, БРАНДМАУЭРЫ. НУ, А ВОООБЩЕ-ТО ЛУЧШЕ ВСЕГО СТАВИТЬ СИСТЕМУ, ПОДДЕРЖИВАЮЩУЮ ИНТЕРНЕТ-МАГАЗИН В ЗАЩИЩЕННОМ DATA-ЦЕНТРЕ, С ЗАЩИЩЕННЫМИ КАНАЛАМИ СВЯЗИ, С ОПЫТНЫМИ СИСТЕМНЫМИ АДМИНИСТРАТОРАМИ И АДМИНИСТРАТОРАМИ БАЗ ДАННЫХ, ЧЬЯ РАБОТА И ЗАКЛЮЧАЕТСЯ В ЗАЩИТЕ И СОХРАНЕНИИ СИСТЕМЫ.

несколько советов по безопасной оплате покупок в Сети

- 1 НЕ ОСУЩЕСТВЛЯТЬ ОПЛАТУ ПЛАСТИКОМ В РАЗЛИЧНЫХ ПОДОЗРИТЕЛЬНЫХ МЕСТАХ — ПОРНО-, ВАРЕЗНЫХ САЙТАХ, САЙТАХ С КРЭКАМИ И ПРОЧЕЙ ДРЯНЬЮ.
- 2 НЕ РАСПЛАЧИВАТЬСЯ КАРТОЙ В МАГАЗИНАХ, ИСПОЛЬЗУЮЩИХ ВИРТУАЛЬНЫЙ ХОСТИНГ. ОБЫЧНО ИХ ХОРОШО ВИДНО ПО ДОМЕННЫМ АДРЕСАМ ТРЕТЬЕГО УРОВНЯ.
- 3 НЕ ОПЛАЧИВАТЬ КАРТОЙ ПОКУПКИ В МАЛЕНЬКИХ ОНЛАЙНОВЫХ МАГАЗИНАХ, ЕСЛИ ОНИ НЕ РАБОТАЮТ С ХОРОШО ИЗВЕСТНЫМИ ПРОЦЕССИНГОВЫМИ СИСТЕМАМИ (ASSIST, CYBERPLAT ИЛИ ПРОЦЕССИНГОВЫЙ ЦЕНТР «ИМПЭКСБАНКА»).
- 4 ДЛЯ ОПЛАТЫ В ИНТЕРНЕТЕ ЗАВЕСТИ ОТДЕЛЬНУЮ ПЛАСТИКОВУЮ ИЛИ ЭЛЕКТРОННУЮ КАРТУ, КОТОРАЯ БУДЕТ ИСПОЛЬЗОВАТЬСЯ ТОЛЬКО ДЛЯ ЭТИХ НУЖД.
- 5 НА КАРТЕ ДЛЯ ОПЛАТЫ ТОВАРОВ И УСЛУГ ЧЕРЕЗ ИНТЕРНЕТ УСТАНОВИТЬ ЛИМИТ ДОСТУПНЫХ СРЕДСТВ.
- 6 НЕ ДЕРЖАТЬ НА КАРТЕ, КОТОРОЙ РАСПЛАЧИВАЕШЬСЯ В ИНТЕРНЕТЕ, КРУПНЫЕ ДЕНЕЖНЫЕ СУММЫ. ЛУЧШЕ ВСЕГО ОСТАВЛЯТЬ СЧЕТ КАРТЫ ПОЧТИ ПУСТЫМ, А ДЕНЬГИ НА НЕЕ ПЕРЕВОДИТЬ НЕПОСРЕДСТВЕННО ПЕРЕД ОПЛАТОЙ.
- 7 В ПОЧТОВОЙ ПЕРЕПИСКЕ НЕ СООБЩАТЬ НИКОГДА И НИКОМУ НОМЕРА СВОИХ КАРТ.
- 8 ПОСТОЯННО ПРОВЕРЯТЬ ВЫПИСКИ ПО КАРТЕ, А ЛУЧШЕ ВСЕГО ПОПРОСИТЬ УВЕДОМЛЯТЬ ТЕБЯ ЧЕРЕЗ SMS ИЛИ ПО ПОЧТЕ О КАЖДОЙ ОПЕРАЦИИ ПО КАРТЕ. СЕЙЧАС МНОГИЕ БАНКИ ПОДДЕРЖИВАЮТ ТАКОЙ СЕРВИС.

ПОСЛЕДНИЙ СОВЕТ: ВЕЗДЕ, ГДЕ ВОЗМОЖНО, ИСПОЛЬЗОВАТЬ ВМЕСТО ПЛАСТИКА ИЛИ ВИРТУАЛЬНЫХ КРЕДИТОК ЭЛЕКТРОННЫЕ ДЕНЬГИ, КОТОРЫЕ СОЗДАНЫ КАК РАЗ ЧТОБЫ УДОБНО И БЕЗОПАСНО ОПЛАЧИВАТЬ ПОКУПКИ В СЕТИ.



электронные деньги E-money были созданы именно для того, чтобы заменить пластиковые карты в интернете. К сожалению, не все магазины и сервисы, особенно западные, принимают электронные средства платежей, а если и принимают, то, как правило, только те виды, которые не распространены в России. Однако сейчас многие российские сервисы и интернет-магазины начинают принимать электронные деньги — воспользуйтесь этим. Ниже перечислю основные виды электронных платежных систем в России.

webmoney (www.webmoney.ru) Не является платежной системой формально (электронные кошельки оперируют с так называемыми титульными единицами), однако она полностью эквивалентна полноценной платежной системе, потому что деньги можно и вводить различными способами, и выводить практически как угодно. Магазины и сервисы, принимающие Webmoney, исчисляются сотнями (www.wmgate.ru).

Впрочем, по той же причине — удобство использования и определенная обезличенность — на Webmoney часто кладут глаз разные жулики. Кладут глаз, конечно, не с точки зрения использования сервиса в своих преступных делах, а просто как на средство оплаты. Мошенник заводит кошелек не указывая данных о себе, рассылает с помощью спама призыв из серии «Извините, что к вам обращаюсь. Сами мы не местные, помогите, кто сколько сможет, — вот кошелек Webmoney.» и ждет щедрых пожертвований.

Webmoney — наиболее защищенная система из всех существующих в России. Кроме того, этот сервис предоставляет на выбор два вида клиентов:

ЧТОБЫ ЗАВЛАДЕТЬ ТВОИМ КОШЕЛЬКОМ, ЗЛОУМЫШЛЕННИК ДОЛЖЕН ЗНАТЬ ТВОЙ ПАРОЛЬ И ИМЕТЬ ВСЕ ФАЙЛЫ КЛЮЧЕЙ

НЕ ДЕРЖИ КРУПНЫЕ ДЕНЕЖНЫЕ СУММЫ НА КАРТЕ, КОТОРОЙ ПОЛЬЗУЕШЬСЯ ДЛЯ ОПЛАТЫ ЧЕРЕЗ ИНТЕРНЕТ

программу-клиент Webmoney Keeper Classic и web-клиент Webmoney Keeper Lite. Web-клиент подходит тем пользователям, которые хотят иметь доступ к своему кошельку в любое время и в любом месте, а Keeper Classic (значительно более защищенный) используют те участники системы, которые, как правило, совершают все операции с одного компьютера.

Webmoney поддерживает работу с несколькими видами валют: доллары, рубли и евро. Обменивать их можно в специальных онлайн-обменных пунктах. Кроме того, можно привязать к Webmoney обычную пластиковую карточку (определенного банка) и использовать ее для ввода/вывода средств с минимальными процентами.

«ЯНДЕКС.ДЕНЬГИ» (money.yandex.ru) Вторая наиболее популярная в России система электронных денег, которая базируется на довольно распространенной в мире технологии PayCash. В отличие от Webmoney, это настоящая платежная система (Яндекс получил банковское свидетельство для системы интернет-платежей от Центробанка).

«Яндекс.Деньги» также предоставляет два вида интерфейса: программу-клиент и защищенный web-интерфейс. В качестве защиты программа-клиент использует пароль и файлы ключей. Однако защиты каждой транзакции с помощью «номера Тьюринга», как в Webmoney, «Яндекс.Деньги» не имеет. Кроме того, эта платежная система оперирует только рублями, а регистрация в системе требует ввода паспортных данных.

Несмотря на довольно простой интерфейс, «Яндекс.Деньги» мало чем уступает Webmoney, а по каким-то параметрам даже превосходит ее. Количество сервисов, которые принимают «Яндекс.Деньги» (money.yandex.ru/shops.xml), составляет несколько десятков, и их число постоянно растет.

деньги@mail.ru система появилась совсем недавно и пока не пользуется особой популярностью. Программы-клиента нет, есть только web-интерфейс. Вариантов ввода и вывода денег из системы меньше, чем в других системах. Список магазинов и сервисов, работающих с этим видом платежей, пока достаточно мал (money.mail.ru/?shops). Однако «Деньги@Mail.ru» имеют довольно удобную возможность — отправку денег на обычный e-mail. Пользователю приходит письмо с сообщением о переводе и предложением создать кошелек (это можно сделать за пять минут), чтобы получить переведенные деньги.

При регистрации можно не сообщать никаких сведений о себе, а только указать e-mail. Однако если тебе понадобится выводить деньги через банковский счет, то, разумеется, потребуются паспортные данные.

механизмы использования электронных денег Электронные деньги — это некий сервис, зарегистрировавшись в котором, ты получаешь свой идентификационный номер. К номеру привязывается твой «электронный кошелек» или «кошельки», если сервис поддерживает различные виды валют. Главный вопрос, который тут же возникает у пользователя, если он только что завел себе подобный «кошелек», — каким образом класть деньги и как можно при необходимости выводить их, то есть обналичивать?

как правило, ввод денег производится следующим образом:

- ЧЕРЕЗ ПРЕДОПЛАЧЕННЫЕ КАРТЫ (АНАЛОГИЧНО ПОПОЛНЕНИЮ СЧЕТОВ СОТОВЫХ ТЕЛЕФОНОВ).
- ПЕРЕВОДОМ С БАНКОВСКОГО СЧЕТА.
- ПЕРЕВОДОМ С ПЛАСТИКОВОЙ КАРТЫ.
- ПОЧТОВЫМ ПЕРЕВОДОМ.
- НАЛИЧНЫМИ В АВТОМАТАХ И БАНКОМАТАХ.
- НАЛИЧНЫМИ В СПЕЦИАЛЬНЫХ ОБМЕННЫХ ПУНКТАХ.
- ОБМЕНОМ С ДРУГИХ ПЛАТЕЖНЫХ СИСТЕМ (КАК ПРАВИЛО, ЭЛЕКТРОННЫХ).

Способы использования электронных денег разнообразны, поэтому с вводом денег в «электронный кошелек» нет никаких проблем. Нужно только по возможности выбирать такие средства, на которых взимаются минимальные

реальный опыт: assist

XS: ЧТО ТАКОЕ ASSIST?

МАРИНА ИСАЕВА, РУКОВОДИТЕЛЬ ОТДЕЛА PR И МАРКЕТИНГА ООО «АССИСТ»: Assist — это шлюз, основные функции которого заключаются в том, чтобы ASSIST получал от магазина описание заказа, затем производил аутентификацию плательщика с помощью банка-эмитента, после чего инициировал снятие денег с карты плательщика банком-эквайером и в итоге сообщал магазину о результатах оплаты. При этом ASSIST обеспечивает защиту данных кредитной карты.

XS: КАКИМ ОБРАЗОМ ОБЕСПЕЧИВАЕТСЯ ЗАЩИТА И КАК ОТСЛЕЖИВАЮТСЯ МОШЕННИКИ?

МАРИНА ИСАЕВА: ASSIST имеет собственную службу мониторинга интернет-транзакций, которая отслеживает платежи мошенников. Кроме того, в 2003 году ASSIST стала первой российской системой электронных платежей, прошедшей совместно с Балтийским банком сертификацию VISA по технологии безопасных платежей 3D-Secure. Для интернет-магазина данная технология делает платежи значительно более безопасными. Магазин, в случае платежа по 3D-Secure, не будет нести потерь в результате действий карточных мошенников, так как аутентификация личности держателя карточки происходит на стороне банка-эмитента. Таким образом, снимается один из основных барьеров, мешающих магазину принимать кредитные карты в интернете. Технология 3D-Secure, по утверждению VISA, на данный момент является наиболее безопасной из всех существующих, а это, безусловно, влияет на конкурентоспособность магазинов и лояльность держателей карточек. Также для обеспечения безопасности владельцев карточек мы реализовали сервис AssistID. 16-значный идентификатор Assist-ID привязан к кредитной карте и используется при оплате товаров или услуг вместо данных реальной карты, защищая тем самым кредитку от ненужного внимания мошенников. На данный момент пластиковые карты ASSIST с эмбоссированными на них AssistID получили более 15 000 человек.

XS: СКОЛЬКО МАГАЗИНОВ ОБСЛУЖИВАЕТ ASSIST?

МАРИНА ИСАЕВА: На данный момент количество обслуживаемых нами магазинов — более восьмисот.

XS: КАКОЙ ОБЪЕМ СРЕДСТВ ПРОХОДИТ ЧЕРЕЗ ВАШУ СИСТЕМУ?

МАРИНА ИСАЕВА: Более миллиона долларов в месяц и порядка \$24 млн. в год. Количество обрабатываемых транзакций по кредитным картам ежегодно увеличивается примерно в 2,5 раза. Медленнее развивается электронная наличность — здесь рост составляет порядка 100% в год.

XS: КАКИЕ ВИДЫ ОНЛАЙНОВЫХ МАГАЗИНОВ ЧАЩЕ ВСЕГО ПОЛЬЗУЮТСЯ УСЛУГАМИ ASSIST?

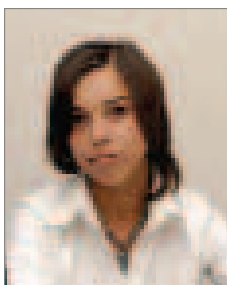
МАРИНА ИСАЕВА: Наиболее перспективными сегментами рынка интернет-магазинов, по данным ASSIST, являются продажа билетов через интернет (причем это билеты как на театральные зрелищные мероприятия, так и авиа- и железнодорожные билеты), книг, CD, DVD, игровых сервисов, продажа цветов, программного обеспечения. Обороты по данным сегментам составляют порядка 50% от общего оборота компании.

XS: ЕСЛИ Я, КАК ВЛАДЕЛЕЦ МАГАЗИНА, РЕШИЛ ВОСПОЛЬЗОВАТЬСЯ ВАШЕЙ СИСТЕМОЙ, ЧТО Я ДОЛЖЕН СДЕЛАТЬ И НАСКОЛЬКО ЭТО ВСЕ СЛОЖНО?

МАРИНА ИСАЕВА: Интеграция платежной системы в сайт интернет-магазина предельно проста и займет у программиста один день. Никакого дополнительного программного обеспечения не нужно. Необходимо только встроить дополнительный код на страницу оплаты. Другое дело, что магазин должен быть готов к введению нового сервиса. Платежи в любом случае должен кто-то отслеживать, плюс нужно понимать, что заказы будут поступать со всего мира, поэтому доставка должна быть на соответствующем уровне.

XS: ПОЛЬЗУЮТСЯ ЛИ УСЛУГАМИ ВАШЕЙ СИСТЕМЫ ОФЛАЙНОВЫЕ МАГАЗИНЫ?

МАРИНА ИСАЕВА: Да, для них мы создали специальную форму оплаты — через V-POS. V-POS — это виртуальный POS-терминал, предназначенный для приема платежей по банковским пластиковым картам в обычном магазине. V-POS представляет собой эмулятор стандартного POS-терминала, через который происходит оплата по карте в обычном магазине. Разница заключается в том, что V-POS, кроме простой оплаты, включает в себя также и все сервисы системы ASSIST. Данное решение реализуется относительно недавно, но уже сейчас видно, что оно становится популярным. Прирост оборота по V-POS составляет порядка 15% ежемесячно.



Марина Исаева, руководитель отдела PR и маркетинга ООО «АССИСТ»

ОТ УСЛУГ МАГАЗИНА, КОТОРЫЙ ПРОЦЕССИТ ТВОЮ КРЕДИТКУ САМОСТОЯТЕЛЬНО, ЛУЧШЕ ОТКАЗАТЬСЯ

ЕСЛИ САЙТ КАЖЕТСЯ ПО КАКИМ-ТО ПРИЧИНАМ ПОДОЗРИТЕЛЬНЫМ, ЛУЧШЕ НЕ РИСКОВАТЬ

проценты (например перевод с банковского счета, с пластиковой карты или наличными).

Средства в «кошельке» ты можешь использовать для оплаты товаров и услуг в интернете. Как я уже писал, почти все электронные магазины в России без проблем принимают подобную «валюту», так что никто не заставит тебя использовать пластиковую карточку там, где это небезопасно.

Почему оплата электронными деньгами гарантированно безопасна? Потому что электронные деньги разрабатывались именно для решения подобных задач и очень серьезно защищены. В отличие от пластиковых карт, номера которых приходится вводить для оплаты (после чего они нередко становятся доступными всем мошенническим ветрам), электронными деньгами можно пла-

тить где угодно и как угодно. Знание номера твоего кошелька, в отличие от номера пластиковой карты, не даст совершенно никаких шансов потенциальному злоумышленнику, и, более того, ты сам можешь сообщать этот номер кому угодно, например чтобы на твой счет перевели деньги.

СХЕМА ЗАЩИТЫ Вот принцип ее работы. Если ты стал участником системы электронных платежей, ты получаешь программу-клиент (впрочем, ее поддерживают не все аналогичные системы). Программа идентифицирует тебя не только по идентификационному номеру в системе, но и по специальным уникальным ключам, которые создаются при настройке клиента и могут храниться на специальных сменных носителях — дискетах, flash'ках и т.д. Кроме того, каждая транзакция требует ввода кода защиты от роботов — на случай если на твой компьютер кто-то подсадит троян и попытается удаленно перевести деньги с твоего компьютера.

таким образом, чтобы завладеть твоим кошельком, злоумышленнику нужно:

1 УЗНАТЬ ТВОЙ ПАРОЛЬ.

2 СКОПИРОВАТЬ ФАЙЛЫ КЛЮЧЕЙ (КОТОРЫЕ МОГУТ БЫТЬ ДОСТАТОЧНО БОЛЬШИМИ, ЧТОБЫ БЫЛО НЕВОЗМОЖНО НЕЗАМЕТНО ПЕРЕДАТЬ ИХ ЧЕРЕЗ ИНТЕРНЕТ).

Даже если мошенник добрался до твоего кошелька, ты в любой момент можешь восстановить полный контроль над деньгами и поменять пароль и файлы ключей, если зарегистрировал кошелек на свои паспортные данные.

Непосредственно в момент оплаты магазин запрашивает у тебя номер кошелька (общедоступный) и направляет соответствующую информацию через платежную систему, которая, в свою очередь, посылает запрос на твой личный кошелек, где ты или подтверждаешь желание перевести средства, или отклоняешь запрос.

Таким образом, при оплате с электронного кошелька магазин в любом случае (и это очень важно) не получает никакой опасной для тебя информации, которой в дальнейшем можно восполь-

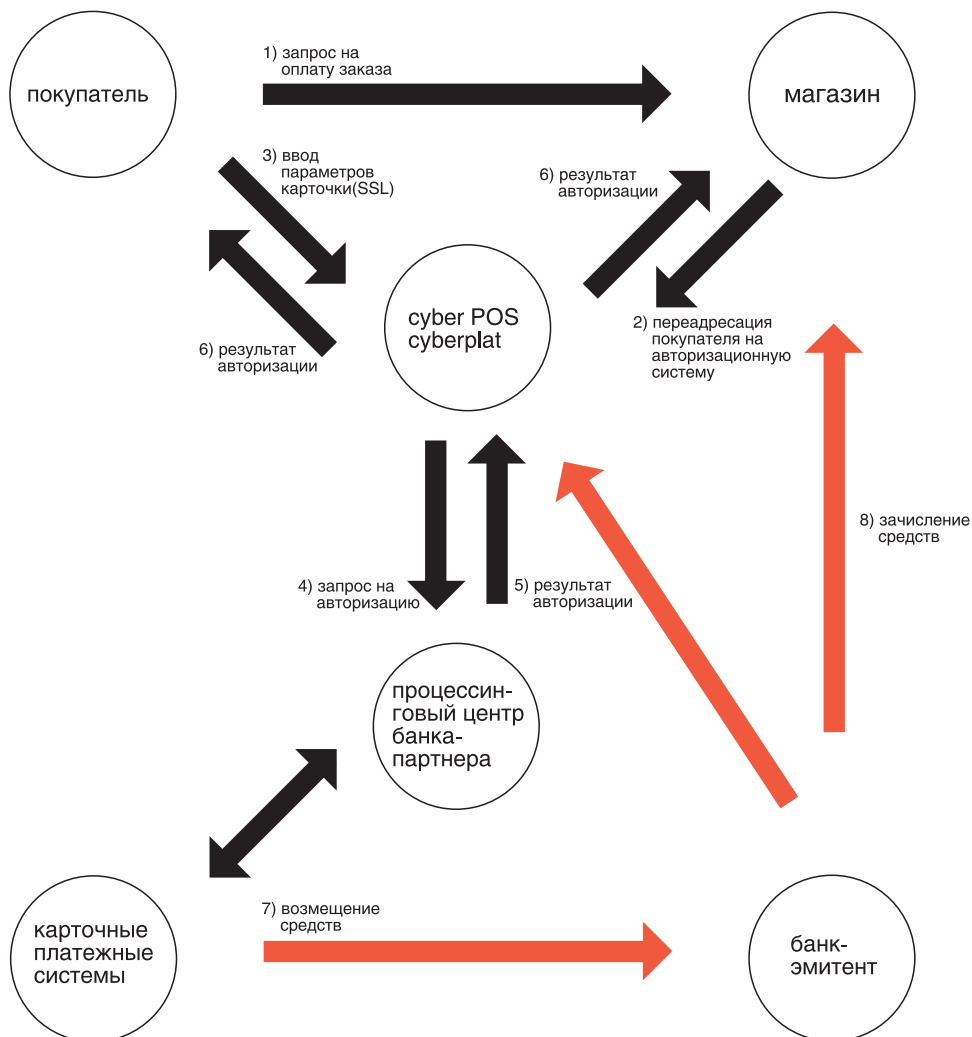
зоваться. При этом и по Сети не передаются никакие важные данные, если ты используешь программу-клиент. Пароль вводится на твоем компьютере, файлы ключей берутся со съемного устройства, для транзакции требуется дополнительное подтверждение (защита от роботов). Этот способ весьма безопасный, особенно по сравнению с оплатой пластиком, при которой сердце так и екает, так и екает...

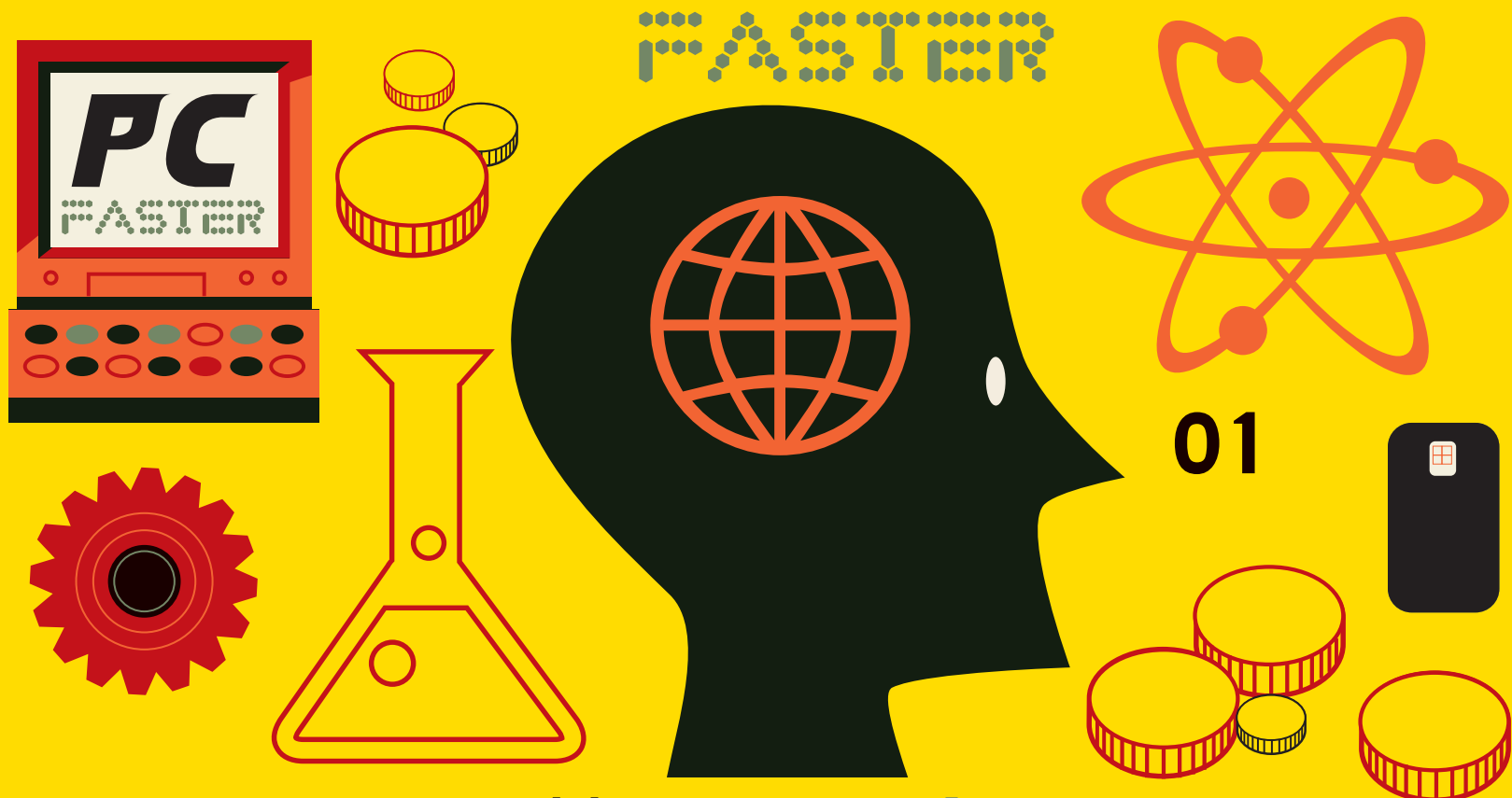
вывод денег из электронного кошелька проводится так же, как и ввод:

- ПЕРЕВОДОМ НА БАНКОВСКИЙ СЧЕТ.
- ПЕРЕВОДОМ НА СЧЕТ ПЛАСТИКОВОЙ КАРТЫ.
- ПОЧТОВЫМ ПЕРЕВОДОМ.
- НАЛИЧНЫМИ В СПЕЦИАЛЬНЫХ ОБМЕННЫХ ПУНКТАХ.
- ОБМЕНОМ НА СРЕДСТВА ДРУГИХ ПЛАТЕЖНЫХ СИСТЕМ (КАК ПРАВИЛО, ЭЛЕКТРОННЫХ).

Ты можешь заводить кошелек совершенно анонимно, но при этом окажутся недоступными многие удобные сервисы: ввод и вывод денег через банковский счет, восстановление контроля над кошельком в случае его утраты и т.д.

Если у тебя есть пластиковая карточка, то самый простой и наименее затратный способ — переводить деньги с нее на электронный кошелек, который будешь использовать для платежей в интернете. В этом случае можно быть совершенно спокойным за сохранность своих сбережений.





СЛОЖНЫЙ СИМБИОЗ

ЧТО ПОЛУЧИТСЯ, ЕСЛИ СКРЕСТИТЬ ПЛАСТИКОВУЮ КАРТУ И WEBMONEY

ОФИЦИАЛЬНАЯ СТАТИСТИКА СВИДЕТЕЛЬСТВУЕТ О ТОМ, ЧТО КОЛИЧЕСТВО ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ПЛАСТИКОВЫХ КАРТ, С КАЖДЫМ ГОДОМ УВЕЛИЧИВАЕТСЯ, А НАНОСИМЫЙ МАТЕРИАЛЬНЫЙ УЩЕРБ ВОЗРАСТАЕТ В АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ. КОМПАНИИ, ОСОБЕННО БАНКИ, СТРЕМЯТСЯ СКРЫТЬ ФАКТЫ КОМПЬЮТЕРНОГО ВОРОВСТВА, ОПАСАЯСЬ ПАДЕНИЯ ДОВЕРИЯ ВКЛАДЧИКОВ, АКЦИОНЕРОВ И ПАРТНЕРОВ

РОМАН КОПЕНЕВ

Ущерб от деятельности кардеров почти не фиксируется в официальной статистике. Жертвы кардеров часто даже не подозревают, что их обокрали. Эксперты полагают, что в США компьютерные мошенники похищают из банков суммы денег, в четыре раза превышающие потери от вооруженных ограблений. Преступления кардеров отличаются простотой, отсутствием насилия, а также тем, что потерпевшие — банк и законный собственник карты — как правило, никогда не видят преступника.

Изначально банковские платежные карты создавались исключительно для офлайн-платежей. Банковская платежная карта — удобное средство для совершения покупок в обычных магазинах или получения наличных в банкоматах. С одной стороны, расплачиваться по банковской карте в Сети достаточно просто и удобно. Банковские карты используются для оплаты товаров и услуг у подавляющего большинства западных и очень многих российских торговых web-порталов. В то же время банковские платежные карты не позволяют производить некоторые простые операции, к примеру переводы с карты на карту. Еще один серьезный минус банковских карт в Сети — тяжелое наследие офлайна в виде операций типа МОТО (mail order telephone order). Суть операций, совершаемых через интернет по банковским картам, заключается в том, что заплатить по карте может не только ее владелец: любой человек, узнавший номер твоей карты,

расплатится твоими деньгами практически в любом интернет-магазине, номер и другие реквизиты карты могут быть элементарно украдены.

Существуют также проблемы с продажей электронных денег по кредитным картам. Не секрет, что кредитки изначально не были предназначены для оплаты через интернет и имеют низкую защищенность от кражи и подделок. Опытные кардеры давно научились обходить установленные «противопожарные» меры. Существующие способы противостоять им снижают количество фродовых (мошеннических) операций, но не могут пресечь их на корню. Однако это не критично для интернет-магазинов, которые принимают оплату с кредитных карт. При небольшом проценте возвратов работа будет оставаться рентабельной, с электронными же деньгами дела обстоят по-другому.

webmoney как кредитка Все началось с того, что платежная система WebMoney Transfer запустила сервис пополнения R-кошельков с кредитных/дебетных карт. «Специалисты» WebMoney, так и не настроив антифродовую систему безопасности окончательно, набрались смелости опубликовать новость на официальном сайте WebMoney о сервисе пополнения WMR-кошельков с помощью кредитных карт. На сайте (<http://credcard2wm.wmtransfer.com>) говорилось о 100% безопасности и идентификации владельца карты. Не прошло и четырех часов после начала работы, как на сервис напал кар-



ВОРОВАТЬ ЭЛЕКТРОННЫЕ ДЕНЬГИ ПРОЩЕ МАТЕРИАЛЬНЫХ, К ТОМУ ЖЕ ОТВЕТСТВЕННОСТИ МЕНЬШЕ.

мошенничества. Как активировать 3-D Secure, спецы WM сами рассказали на сайте <http://credcard2wm.wmtransfer.com> в разделе «О сервисе». Следуя описанным там действиям, практически на любой карте из штатов 3-D Secure включался за пять минут. Если карта кредитная, было достаточно просто найти SSN (социальный номер страхования) — такая услуга в Сети стоит \$2-3. Если же карта дебетная, то 3-D Secure включался и без SSN. Таким образом, у кардеров опять появилась возможность скачивать халявные WMR в больших количествах. Единственная загвоздка заключалась в том, что на один персональный Кеепер можно было «залить» максимум 8400 WMR, причем только раз в неделю. Разумеется, Тольяттинским кардерам не составило труда обойти эту антифродовую систему... Появилось несколько вариантов обхода системы безопасности WebMoney:

1 НА ПЕРСОНАЛЬНЫЙ АТТЕСТАТ МОЖНО ВЫВОДИТЬ 60000 WMR В СУТКИ (ЛИМИТ СЕРВИСА).

ДЕЙСТВОВАТЬ ПОШАГОВО НЕ НУЖНО, ДОСТАТОЧНО ДОЙТИ ДО МОМЕНТА ВБИВАНИЯ КАРТЫ СРАЗУ В 10-15-ТИ ОКНАХ, ЗАТЕМ ВБИТЬ ВО ВСЕ ПОЛЯ РАЗНЫЕ КАРТЫ И НАЖАТЬ «ДАЛЕЕ», ТАКИМ ОБРАЗОМ ЗАЧИСЛИВ НА СВОЙ КЕЕПЕР НЕ 8400, А ВСЕ 60000 WMR.

2 НА ЛЮБЫЕ АТТЕСТАТЫ, ДАЖЕ НА ФОРМАЛЬНЫЕ, МОЖНО ЗАЛИВАТЬ 60000 WMR В СУТКИ.

СЛЕДОВАТЕЛЬНО, МОЖНО БЫЛО ЗАЛИВАТЬ КЕЕПЕР'Ы, ВООБЩЕ НЕ ИМЕЮЩИЕ АТТЕСТАТА, ДЛЯ ЧЕГО В ОПЦИЯХ ВЫБИРАЛИ ТИП КАРТЫ НЕ 3-D SECURE, А EWALLET (АЛЬФА-БАНКОВСКИЕ КАРТЫ), И НАЖИМАЛИ «ДАЛЕЕ». ПОСЛЕ ОКОНЧАНИЯ ФОРМИРОВАНИЯ НОМЕРА ЗАКАЗА СТРАНИЦА СОХРАНЯЛАСЬ, И В НЕЙ МЕНЯЛАСЬ ОДНА-ЕДИНСТВЕННАЯ ССЫЛКА, УКАЗЫВАЮЩАЯ НА ПРОЦЕССИНГ 3-D SECURE, А НЕ EWALLET «АЛЬФА-БАНКА».

Благодаря этим оплошностям кардеры вывели около 1500000 WMR! Сервис в данный момент не работает и вряд ли будет работать :). Перечисление на WM-счет с кредитных карт прекратили через два месяца после начала работы сервиса, так как была раскрыта совершенно прозрачная схема мошенничества с номерами кредитных карт: с ворованных карточек на WM-счет перечислялись деньги, после этого — на анонимный счет IMTB, а дальше куда угодно.

анонимность: преимущество или недостаток? Аноним-

ность во взаиморасчетах в системе WebMoney и IMTB можно рассматривать двояко. С одной стороны, для покупателя выгодно быть анонимным: совершаешь разнообразные покупки, при этом скрываешь свою темную личность и не боишься привлечь внимание к себе. Для продавца же анонимность открывает возможности ухода от налогов. С другой стороны, у недобросовестных продавцов появляется возможность не оказывать оплаченные покупателем услуги. Соответственно, покупатель оказывается неспособным (при утере секретных ключей для доступа к электронному кошельку) получить доступ к оставшимся на счету средствам и доказать свои права на них.

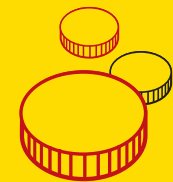
Кардеры выводят деньги с ворованных кредиток на WebMoney с удовольствием — это идеальный способ превращения денег на ворованных кредитках в наличность. Даже привязка кредитной карты к WM-аттестату (не ниже персонального) не помогла: кардеры стали оформлять аттестаты на подставных лиц, использовать временные телефонные номера и т.д.

В общем, использовать кредитную карту для расчетов в интернете без дополнительных мер нежелательно, а кое-где и просто невозможно. Но не подумай, что кредитная карта не может участвовать в различных схемах электронных платежных систем. К тому же у кредитки есть существенные для интернета достоинства: широкая распространенность и интернациональность, возможность расплачиваться практически в любой валюте, чего не скажешь о WebMoney.

дер, который, по данным Арбитражной системы WebMoney, успел выкачать около \$4000, что примерно равно 120000 WMR.

Действия кардера были простыми. Получить формальный аттестат WebMoney, который выдается автоматически при заполнении определенных полей, и кредитную карту, которых у кардеров сотни. Злоумышленник прошел авторизацию своего WM-кипера, заполнил поля данными кредитной карты, нажал «Далее» и через 15 секунд на его Кеепер зачислилась сумма в 4500 WMR. А дальше — монотонный труд :). И вот пробило семь утра по Москве, «специалисты» WebMoney проснулись, раскрыли рты от подобных движений и отрубили сервис — потом в течение недели при заходе на <http://credcard2wm.wmtransfer.com> выдавалась ошибка 404 Not Found. А кардер успел вывести \$4000 через «Израильский обменный пункт» с помощью Western Union.

После этого эксцесса пополнять свой WM Кеепер стало возможно только при наличии персонального аттестата и кредитной картой с активированной поддержкой 3-D Secure, которая якобы снова предоставляла 100% гарантию спасения от



WEBMONEY — ДЛЯ КАРДЕРОВ ОТЛИЧНЫЙ СПОСОБ ВЫВОДИТЬ ДЕНЬГИ С ВОРОВАННЫХ КРЕДИТОК.

СЕРВИС ПОПОЛНЕНИЯ R-КОШЕЛЬКОВ С КРЕДИТНЫХ/ДЕБЕТНЫХ КАРТ БЫЛ ВЗЛОМАН В СЧИТАННЫЕ ЧАСЫ.



кардинг ПО-НОВОМУ

СОВРЕМЕННЫЕ МЕТОДИКИ ВЗЛОМА

ОДНИ ХАКЕРЫ ЛОМАЮТ ПРОГРАММЫ, ДРУГИЕ — ПЛАТЕЖНЫЕ СИСТЕМЫ: НЕ ВЛАМЫВАЯСЬ, КАК ГРАБИТЕЛИ, СРЕДИ БЕЛА ДНЯ И НЕ КРИЧА «РУКИ ВВЕРХ!», ДЕЙСТВУЮТ СКРЫТНО И ЗАМЕТАЮТ СЛЕДЫ. НАЙТИ ТАКИХ ЛЮДЕЙ ОЧЕНЬ ТРУДНО. ХОЧЕШЬ УЗНАТЬ, КАК РАБОТАЮТ РЕАЛЬНЫЕ КАРДЕРЫ? | КРИС КАСПЕРСКИ АКА МЫШЦЬХ

Давным-давно, когда никакого интернета даже в проекте не было, народ уже вовсю начал пользоваться кредитными картами. Проверка подлинности кредитки представляла большую проблему: при каждой покупке звонить в банк и проверять состояние счета клиента магазинам не позволяли технические ресурсы и стоимость междугородных звонков (в то время существенно выше цены пары пачек сигарет или бутылки колы). Существовал определенный порог для денежных сумм, ниже него проверка подлинности не производилась, а продавец верил клиенту на слово (конкретное значение порога каждый ма-

газин выбирал самостоятельно). Подделать карту, не имея специального (и весьма дорогостоящего) оборудования было очень сложно. И хотя существовала вероятность купить трехтомник Кнута за \$50 при балансе на карте всего в \$10 или даже \$1, поиск злоумышленника не представлял особого труда (карты выдаются не просто так, а только тем, у кого есть счет в банке).

Появление интернет-магазинов породило множество проблем. Удаленный сервер не может «пощупать» кусок пластика и видит лишь последовательность цифр, определяющую номер карты. Разумеется, комбинация цифр

ПОДДЕЛАТЬ КАРТУ (САМ ПЛАСТИК) БЕЗ СПЕЦИАЛЬНОГО ОБОРУДОВАНИЯ ОЧЕНЬ СЛОЖНО.

ДЛЯ ПОКУПКИ В ИНТЕРНЕТ-МАГАЗИНЕ ПЛАСТИКОВАЯ КАРТА НЕ ПОТРЕБУЕТСЯ — ДОСТАТОЧНО ПОСЛЕДОВАТЕЛЬНОСТИ ЦИФР.

ЧТОБЫ ВЗЛОМАТЬ ИНТЕРНЕТ-МАГАЗИН, НУЖНО ЗАБРОСИТЬ СВОЙ ШЕЛЛ-КОД НА УДАЛЕННЫЙ УЗЕЛ. КАК — БЕЗ РАЗНИЦЫ.

не случайна и не любая из них будет воспринята с благодарностью. В номер карты прежде всего входит контрольная сумма, страхующая от ошибки набора, а также некоторая другая информация (тип банка-эмитера, тип самой карты и т.д.). Взять и ввести что-нибудь от балды не получится: тебе откажут. Однако если расшифровать алгоритм кодирования номеров, можно сгенерировать вполне правдоподобный номер, который визуально ничем не отличается от подлинного. Конечно, магазин может послать в банк запрос: «А существует ли такой номер вообще?» Но... это же пока придет ответ! А цивилизованный клиент ждать не любит :), он просто пожмет плечами и пойдет в другой магазин. Конкуренция!

Алгоритм кодирования номеров долгое время держался в строжайшем секрете, а расшифровать его по одним лишь номерам карт было практически невозможно, поэтому карты быстро завоевали популярность и получили массовое распространение. Незрелость систем связи существенно затрудняла распространение хакерской информации, и если даже кто-то (например уволенный банковский работник) был готов рассказать, что и как, это никому не вредило, так как круг вовлеченных людей был очень мал. С появлением BBS все изменилось. Алгоритм кодирования просочился в массы, хакеры создали множество автоматических генераторов, некоторые из которых живы до сих пор (правда, уже не работают).

Любой подросток мог скачать генератор с клавиатуры и забыть, что такое отсутствие карманных денег. Ущерб от краж стремительно возрастал, но банки долгое время делали вид, что ничего не происходит, дескать, их система прочна, как бронепоезд. Кардерами занималась полиция. Заказы приходили по реальным адресам, и хотя можно было до некоторой

степени замаскировать их (например оформить посылку на имя друга), спрятать хвосты в воду полностью не удавалось. В то же время кражи из-за рубежа (особенно из России) проходили спокойно и безнаказанно. Поимка жулика требовала слишком много юридической волокиты, и у чиновников была всегда наготове железная объяснительная: «У нас тут лю-

Когда снимаешь, не всегда уверен, что не последнее



ЖИЗНЬ СМАРТ-КАРТЫ

1 производство компонентов

ПОСЛЕ СБОРКИ В ЧИП ЗАКЛАДЫВАЕТСЯ СПЕЦИАЛЬНЫЙ КЛЮЧ (КФ). ОН НЕ ПОЗВОЛЯЕТ ВНЕСТИ В НЕГО ИЗМЕНЕНИЯ ДО НЕПОСРЕДСТВЕННОГО ЗАПЕЧАТЫВАНИЯ В ПЛАСТИК. КФ СОЗДАЕТСЯ С ПОМОЩЬЮ АЛГОРИТМОВ И С ИСПОЛЬЗОВАНИЕМ МАСТЕР-КЛЮЧА ИЗГОТОВИТЕЛЯ, КОТОРЫЙ УНИКАЛЕН ДЛЯ КАЖДОЙ КАРТЫ.

2 до персонализации карты

ГОТОВЫЙ ЧИП ПОСТАВЛЯЕТСЯ КОМПАНИИ, ВЫПУСКАЮЩЕЙ ЧИСТЫЕ СМАРТ-КАРТЫ. НА МЕСТЕ ОН УСТАНОВЛИВАЕТСЯ НА ПЛАСТИКОВУЮ ОСНОВУ И ТЕСТИРУЕТСЯ. КФ ЗАМЕНЯЕТСЯ НА КЛЮЧ ПЕРСОНАЛИЗАЦИИ (КР), ДЛЯ ДОПОЛНИТЕЛЬНОЙ БЕЗОПАСНОСТИ НА КР УСТАНОВЛИВАЕТСЯ БЛОК VPER (PERSONALISATION LOCK). ФИЗИЧЕСКИЙ ДОСТУП К ПАМЯТИ ПОЛНОСТЬЮ ЗАКРЫВАЕТСЯ, А ДЛЯ ЗАПИСИ И ИЗМЕНЕНИЯ ИНФОРМАЦИИ ИСПОЛЬЗУЕТСЯ ТОЛЬКО ПРОГРАММНЫЙ МЕТОД. ПОСЛЕ ЭТОГО СИСТЕМНЫЕ ОБЛАСТИ, НА КОТОРЫХ СОДЕРЖАТСЯ ЗАЛОЖЕННЫЕ КЛЮЧИ, НЕДОСТУПНЫ ДЛЯ ЧТЕНИЯ И ЗАПИСИ.

3 персонализация карты

ЭТОТ ЭТАП ВЫПОЛНЯЕТСЯ КОМПАНИЕЙ-ЭМИТЕНТОМ (НАПРИМЕР БАНКОМ). В ПАМЯТЬ ЗАПИСЫВАЕТСЯ СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, ФОРМИРУЮТСЯ ФАЙЛЫ ДАННЫХ, СОДЕРЖАЩИЕ ИНФОРМАЦИЮ О ВЛАДЕЛЬЦЕ КАРТЫ, PIN-КОДЕ И Т.Д. В КОНЦЕ ДАННЫЕ ЗАКРЫВАЮТСЯ БЛОКОМ VUTIL (UTILISATION LOCK). ПОСЛЕ ЭТОГО КАРТА МОЖЕТ ВЫДАВАТЬСЯ ЕЕ НОВОМУ ВЛАДЕЛЬЦУ.

4 использование карты

В ПРОЦЕССЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММЫ ОБРАЩАЮТСЯ К ЛОГИЧЕСКОЙ ФАЙЛОВОЙ СИСТЕМЕ, ЗАПУСКАЮТ МЕХАНИЗМЫ ШИФРОВАНИЯ И Т.П. ДОСТУП К ДАННЫМ ОПРЕДЕЛЯЕТСЯ ЗАЛОЖЕННОЙ ПОЛИТИКОЙ БЕЗОПАСНОСТИ.

5 истечение срока действия

ПРОГРАММА ЗАПИСЫВАЕТ ПОСЛЕДНИЙ БЛОК (INVALIDATION LOCK) НА МАСТЕР-ФАЙЛ. ПОСЛЕ ЭТОГО ЛЮБЫЕ ОПЕРАЦИИ ЗАПИСИ СТАНОВЯТСЯ НЕДОСТУПНЫ, НО ОПЕРАЦИИ ЧТЕНИЯ МОГУТ БЫТЬ ПРОВЕДЕНЫ, НАПРИМЕР, ДЛЯ АНАЛИЗА ХРАНЯЩЕЙСЯ ИНФОРМАЦИИ. ДРУГОЙ СПОСОБ ЗАКЛЮЧАЕТСЯ В УСТАНОВКЕ БЛОКА НА PIN-КОД И ДОПОЛНИТЕЛЬНЫЙ РАЗБЛОКИРУЮЩИЙ PIN-КОД. В ЭТОМ СЛУЧАЕ СТАНОВЯТСЯ НЕВОЗМОЖНЫ ВСЕ ОПЕРАЦИИ, ДАЖЕ ЧТЕНИЕ.

дей на улицах режут, а вы со своими кардерами». Конечно, кое-кого все-таки ловили и вроде бы даже судили условно, но пойманных — единицы из тысяч! В настоящее время генераторы практически полностью утратили свою актуальность, поскольку почти все интернет-магазины (и, естественно, банки) всегда проверяют подлинность карты, отправляя запрос в банк, тем более что современные технические средства это позволяют.

Вот другой пример «исторического» взлома. Каждый, наверняка, видел, как в фильмах крутые перцы вставляют в банкомат какое-то устройство, на экране бегут цифры, и вот перец достает пачку хрустящих купюр. Что это такое? Оказывается, это генератор PIN-кодов, подключаемый в обход клавиатуры банкомата. Подобрать полный номер кредитки нереально, это займет слишком много времени и будет слишком наглядно: на банк обрушится лавина запросов, банкомат будет немедленно заблокирован. Однако если подсмотреть номер чужой карты, то подобрать PIN вполне реально, если, конечно, делать это не вручную, а с помощью электроники. Банкоматы, естественно, предусматривают блокировку карты после определенного количества неправильных попыток, но в древности защитная схема была плохо отработана и ее удавалось обойти. Теперь все это в прошлом. Очевидные дыры давно заткнуты и просто так не взламываются, в то же время кардеры не сдаются и, можно сказать, их дело процветает.

тайники электронных магазинов Совершая покупку по кредитке, ты неизбежно «засвечиваешь» ее номер. Многие магазины сохраняют его в специальной базе на тот случай, когда ты вдруг придешь еще раз и тем самым, как постоянный покупатель, заслужишь скидку. Разумеется, это не единственная причина для сохранения номеров карт.

Нас уверяют, что никакие данные о нас никому не передаются и не используются во вред нам. Может быть, это действительно так, может быть, действительно налоговые органы удерживаются от соблазна порыться в готовой базе и устроить серьезную разборку: «Как это так? Человек платит \$10 налогов, а каждую неделю совершает покупок на \$10 000». Ясно только одно: если эта база как-то взаимодействует с интернетом, она изолирована от внешнего мира не полностью, соответственно, можно проникнуть в нее и похитить реальные номера кредитных карт, которые выдержат любую проверку.

Конкретные методики взлома могут варьироваться от атаки на операционную систему, под которой вращается сервер, до «инъекции» SQL/PHP-команд в строку формы запроса. Главное — забросить свой shell-код на удаленный узел, а все остальное, как говорится, дело техники. Подробнее об этом можно прочитать, например, в «Записках исследователя компьютерных вирусов» (электронная копия лежит на ftp://nezumi.org.ru).

Пресса регулярно сообщает о том, что у очередного арестованного хакера обнаружены сотни и даже тысячи краденых номеров. Естественно, когда преступник взламывает базу, какой для него смысл уносить с собой только ее часть? Если уж брать, так все. Вот хакеры и берут, тем более что интернет-каналы у них по-настоящему скоростные. Правда, воспользоваться награбленным удастся далеко не всегда и не всем. Дело в том, что если владелец оригинальной карты обнаружит недостаток средств и побежит в банк, карта будет немедленно заблокирована и при первом же обращении с такой карты полиция побежит искать мошенника по адресу, указанному при совершении покупки, к примеру в интернет-магазине. Обналичить деньги через банкомат также не получится, поскольку банкомату требуется «живая» карта, а не только ее номер (как раз карты у похитителя нет). Так что вероятность и опасность подобных краж все-таки сильно преувеличена. Во всяком случае, ни одному хакеру так и не удалось разбогатеть. Прямо как в анекдоте: теоретически мы миллионеры, а практически можем купить только пиво, да и то не без риска.

Правда, есть люди, которые занимаются обналичиванием ворованных денег, естественно, удерживая за это свой процент, который колеблется от 30% до 60% от общей суммы. Но таких людей немного, к тому

где черпали

для ПОДГОТОВКИ ЭТОГО МАТЕРИАЛА МЫ ОБЩАЛИСЬ С ЗАРУБЕЖНЫМИ КАРДЕРАМИ, ТАК КАК НАШИ В ЭТОЙ ОБЛАСТИ НЕ СЕКУТ НИЧЕГО (ИЛИ СЕКУТ, НО МОЛЧАТ, КАК ПАРТИЗАНЫ). ИСПАНИЯ, НИДЕРЛАНДЫ, ШВЕЦИЯ, АВСТРАЛИЯ... ГОВОРИЛИ СО МНОГИМИ И УЗНАЛИ ВПОЛНЕ РЕАЛЬНЫЕ РЕЦЕПТЫ ВЗЛОМА.



В ТЕОРИИ ХАКНУТЬ БАНКОМАТЫ НЕВОЗМОЖНО, НА ПРАКТИКЕ ВСЕ ЗАВИСИТ ОТ ХАЛТУРЫ ТЕХ, КТО ОБСЛУЖИВАЕТ ИХ.

же никто из них не гарантирует хакеру какой бы то ни было «безопасности» — слишком рискованный для него бизнес, лучше не связываться. Намного проще и безопаснее пойти торговать бананами :).

ШПИОНАЖ за соседями При заполнении формы на сайте интернет-магазина вся конфиденциальная информация должна передаваться по специальным протоколам, гарантированно устойчивым к перехвату (например по SSL). Однако некоторые магазины пренебрегают этим требованием, и номер карты передается по сети открытым текстом. Можно ли перехватить его? Теоретически возможно, практически же... Тоже возможно, но для этого придется попотеть.

Начнем с того, что даже если ты захватишь один из промежуточных маршрутизаторов (уже огромная проблема!), выделить жалкие несколько цифр из общего потока гигабайтного трафика, скорее всего, не удастся. Если же атаковать сам интернет-магазин, то ничего перехватывать вообще не нужно. Просто взять базу и уйти!

А вот в локальной сети выловить кое-что все-таки можно. Достаточно установить сниффер и грабить весь пролетающий трафик. Пассивные снифферы грабят только текущий сегмент, активные — и все остальные. В крупных организациях (локальная сеть до сотни узлов, сотрудники из разных отделов даже не знакомы друг с другом) подобные кражи случаются достаточно часто. Вася покупает в интернет-магазине новый диск или регистрируется на порносервере, чтобы немного отвлечься от работы, а Петя ворует номер его кредитки и дальше использует ее по своему усмотрению. Чаще всего Вася не стремится раздувать большой скандал, поскольку ему может достаться. Да и доказать, что кредитку своровал именно Петя, а не кто-то еще, практически невозможно, особенно если Петя использовал ее для доступа на другой порносайт, например с голыми мужиками :). Пускай они ему совершенно фиолетовы, но сам факт! Пусть Вася докажет, что это не он гей. А Петя тем временем будет покупать диски и прочую мишуру...

Аналогичным образом можно действовать и в сетях кабельного интернета, который чаще всего строится на обычном Ethernet. Про беспроводные сети и точки доступа не стоит и говорить — их ломают только так!

оббитый проводами А что насчет банкоматов? Можно ли хакнуть их? На первый взгляд, нет, потому что они оборудованы камерами слежения и соединены с банком выделенным бронированным кабелем, закопанным глубоко под асфальт, причем протокол передачи заведомо устойчив к перехвату. И даже если ты сможешь врезаться в линию банкомат-банк, то не получишь существенных шансов. Максимум — ты просто устоишь тотальный DoS, нарушив работу банкомата, но денежек все равно не получишь. На самом деле все это не более чем теория. Реальные хакеры рассказывают, что в действительности сплошь и рядом для передачи данных используются готовые каналы связи, в том числе телефонные линии и интернет. Сам кабель по пути своего следования заходит то в один, то в другой распределительный шкаф. И самое главное — протокол обмена все-таки неустойчив к перехвату.

Поскольку вся система проектировалась в те далекие времена, когда процессоры мощнее чем Intel 4004 стоили огромную кучу денег и занимали целый шкаф, разработчики просто не могли использовать «тяжелые» алгоритмы шифрования, которые современные компьютеры взламывают за считанные минуты. Но дело даже не в этом. Хакеры нашли эффективные способы повторного снятия денег даже без знания ключа. Приблизительная картина такая. В ходе совершения транзакции банк и банкомат обмениваются зашифрованными пакетами, содержащими, помимо всего прочего, поле синхронизации — 16-битное число, которое увеличивается на единицу с каждым отправленным/принятым пакетом. Поскольку оно зашифровано, предсказать или подделать

Сверху вниз:
Она успела снять зарплату — повезло
Подделанные карточки с виду ничем не отличаются от обычных



его невозможно. Можно только... сбить счетчик синхронизации, пошлав несинхронный пакет. Несмотря на наличие поля контрольной суммы, поле синхронизации в него не попадает, а поскольку здесь используется простейшее потоковое шифрование, искажение поля синхронизации никак не воздействует на остальные поля, соответственно, такой пакет будет воспринят банкоматом как правильный. Однако счетчик синхронизации будет сброшен, следовательно, ты сможешь повторить посылку посланных ранее пакетов, перехваченных до этого. И банкомат послушно снимет деньги с карты еще раз. Естественно, чтобы поля синхронизации совпали, необходимо сбрасывать счетчик до начала легального снятия денег клиентов и перед повтором этой операции. Поскольку число повторов ограничено только количеством денег на счету жертвы, абсолютно неважно, сколько снимать: один доллар или сто. Можно снять сколько угодно!

Основная проблема — способ перехвата канала связи. Конечно, можно залезть в распределительный шкаф, предварительно сорвав замок, но это совсем не по-хакерски. В случае с телефонной линией все проще. Цифровые АТС неплохо исследованы хакерами и имеют множество дыр, через которые можно подключиться к любому каналу. Про интернет вообще не стоит и говорить: взломать провайдера хоть и сложная, но вполне решаемая задача.

летучие голландцы Вместо того чтобы обчищать чужие магазины, многие жулики создают свои. В Штатах и Европе эта деятельность идет на широкую ногу и буквально ошеломляет своим размахом. Такое впечатление, что жульничество в конце XX века стало нормой жизни.

Некоторые (и их меньшинство) просто подыскивают раскрученный интернет-магазин или любой другой сайт, работающий с кредитками (например порно), создают его визуальную копию, размещают ее на близком по написанию домене так, чтобы те, кто ошибся в написании, попали в загребущие лапы. Остается просто считать номер кредитки и отправить клиента ожидать заказа, который ему, естественно, не придет. Или... все-таки придет? Некоторые жулики, рассчитывая на долговременный бизнес, действительно высылают заказ, усыпляющий бдительность клиента, а через некоторое время обчищают его счет до последнего цента.

Как вариант, можно прибегнуть к массовой рассылке с предложением перейти по ссылке. Маловероятно, чтобы все пользователи вчитывались в ее написание, тем более что дырявый Outlook Express позволяет легко маскировать ссылки. Человек думает, что переходит к сайту А, а на самом деле его направляют на сайт В.

Еще можно внедриться в файл hosts, хранящий IP-адреса некоторых доменных имен, одна-

Сунуть — полдела, надо еще снять

ко для этого хакеру необходимо получить статус администратора на атакуемой машине, но разве это проблема? Рассылаешь заманчивый файл, не открыть который просто невозможно, и пожинаешь урожай.

Впрочем, все эти пути незаконны и небезопасны. А вот вполне честный путь. Человек покупает у тебя, скажем, пачку сигарет за \$6, а с его карточки каждый месяц снимается \$100. Как? За что? Почему? Никто никого не грабит. \$100 — за льготную подписку на журнал о вкусной и здоровой пище. Было же сказано в 200-страничном соглашении, что все покупатели автоматически получают членство... Ага, вон там на 110-й странице мелким шрифтом. Кто не прочитал, сам виноват :). Ты ничего не воруюшь, ты ведешь честный бизнес, а за наезды еще и в суд можешь подать: «Уйдите и не отвлекайте службу поддержки своими дурацкими вопросами :»).

Покупаешь в магазине диск своей любимой группы. Через месяц получаешь внушительную посылку, в которой помимо диска много всего... Вот, думаешь, как же здорово на Западе магазины работают. Столько бонусов за первую покупку. Как же, бонусы. Это был реальный товар, который тебе всучили, воспользовавшись тем, что тебе было лень читать все написанное. И главное — не придерешься. Все предельно честно.

Многие люди склонны считать, что воруют в основном на порносайтах. Но не все порносайты созданы жуликами, и, наоборот, не все не порносайты созданы честными людьми. Часто бывает так.

социальная инженерия Среди множества объявлений, предлагающих работу, часто попадаются вполне приемлемые варианты. Тебя готовы принять в любое время, только предварительно необходимо завести кредитную карту, на которую будет поступать зарплата. И, естественно, сообщить ее номер для проверки, а то ведь мало ли что... Если такая карта у тебя уже есть, то это вообще хорошо! Стоит ли говорить, что далее «фирма» снимает все твои деньги и исчезает, а ты даже не знаешь, к кому идти жаловаться. Никто не будет искать виртуальную фирму, существующую только в электронных проводах и сетевых картах.

Список методик «безболезненного» отъема денег довольно обширен и разнообразен. Далеко не всегда удается удостовериться, что имеешь дело с обманщиком. Например, тебе предложили 100% работающий генератор номеров (не троян) за... \$1000. А как ты хотел? Настоящие генераторы обычно стоят даже дороже. Вот несколько сгенерированных наугад номеров. Проверь их — они работают! Интернет-магазины принимают их к оплате. Да нет же, это не троян. Я точно говорю. Вот исходные тексты, вот откомпилированный файл. Смотри: никакого подвоха тут нет, и воровать с твоего компьютера никто ничего не собирает. Ну и так далее, в том же духе, пока клиент не выложит \$1000 за совершенно бесполезную программу. Да, в нее вложена толпа реально работающих номеров. Но все это — кредитные карты злоумышленника. Естественно, они работают! В смысле, они отовариваются. Правда, на них лежит совсем немного денег, и сразу же после сделки злоумышленник немедленно блокирует все карты, так что покупатель остается с носом. Вот такое наказание за жадность. А кому жаловаться? «Я купил генератор и только собрался похакерствовать, как обнаружил, что меня кинули на \$1000. Гражданин прокурор, разберитесь с ними, пожалуйста!». Смешно? Конечно, чисто теоретически обиженный покупатель может нанять братков, но это уже совсем другая история.

а стоит ли? Мошенничество с кредитными картами совершается ежедневно, и кардеры не собираются сдавать своих позиций. Напротив, они наступают, занимают все новые и новые территории. Однако. Я никогда не занимался кардерством, поскольку оно подошло слишком близко к обыкновенному воровству, за которым не стоит никакого исследовательского духа. Только стремление к деньгам и жажда наживы, а настоящие хакеры в первую очередь стремятся к знаниям!

ИНОГДА НАПИШУТ МЕЛКИМ ШРИФТОМ — И ВРОДЕ БЫ РАМКИ ЗАКОНА НЕ НАРУШЕНЫ.

ПОПУЛЯРНЫЙ СПОСОБ ПОДЗАРБОТАТЬ — СДЕЛАТЬ КОПИЮ РЕАЛЬНОГО РЕСУРСА И РАЗМЕСТИТЬ ЕГО НА СОЗВУЧНОМ ИЛИ ИМЕЮЩЕМ «ОШИБКУ» В НАПИСАНИИ ДОМЕНЕ.



атака на смарт-карты

БЕЗОПАСНОСТЬ ПЛАТЕЖНЫХ СМАРТ-КАРТ

ОБЛАСТИ ПРИМЕНЕНИЯ СМАРТ-КАРТ МНОЖЕСТВЕННЫ, В ТОМ ЧИСЛЕ ХРАНЕНИЕ ДАННЫХ (STORED VALUE CARD), КОТОРЫЕ МОЖНО ИСПОЛЬЗОВАТЬ В ЭЛЕКТРОННОЙ КОММЕРЦИИ, ТО ЕСТЬ ДЛЯ ОПЛАТЫ ПОКУПОК ЧЕРЕЗ ИНТЕРНЕТ. ПОСМОТРИМ, НАСКОЛЬКО НАДЕЖНЫ СМАРТ-КАРТЫ | **АНДРЕЙ МЕЖУТКОВ**

неагрессивные атаки на смарт-карту Предотвратить неагрессивные атаки, или атаки на канал (например пассивное прослушивание протокола обмена атакующим), крайне трудно. Атаки на канал используют изменение и анализ аналоговых характеристик при работе карт, то есть изменение потребления мощности, изменение уровня излучения какого-то элемента при выполнении микропроцессором карты каких-либо операций.

Самая простая атака — это блокирование доступа для ридера к соответствующему контакту на карте. Подобная атака часто применялась к картам доступа платного телевидения. Блокировался вход, через который телекомпания подавала сигнал о прекращении показа неоплаченного канала.

Если заблокировать этот контакт куском скотча или подключить к нему диод, то снова можно будет смотреть все каналы. Аналогично были «доработаны» карты для телефонов-автоматов. Контакт, который уменьшает сумму на этой предоплаченной карте, специально загрязнялся или вообще отламывался, и карта становилась «вечной». Однако сегодня очень немного смарт-карт, в которых такая уязвимость не ликвидирована.

Еще один вид атак, временной анализ, основан на том, что оценивается время выполнения смарт-картой какой-либо операции. Если атакующий имеет физический доступ к карте и может делать подобные измерения, то сможет использовать полученные данные для вычисления ключа карты. Известный крип-



АТАКИ НА СМАРТ-КАРТЫ ДЕЛЯТ НА АГРЕССИВНЫЕ И НЕАГРЕССИВНЫЕ (ПАСИВНЫЕ)

тоаналитик Пауль Кочер, тот самый, который показал слабость шифра в архиваторе PkZIP, опубликовал результаты своих исследований о временной атаке на смарт-карту в декабре 1995 года. Простой и эффективный способ противодействия такой атаке — вводить нелинейные задержки при использовании ключевой информации.

Простой анализ потребляемой мощности, дифференциальный анализ и дифференциальный анализ высокого порядка становятся возможными из-за того, что при работе смарт-карты изменяются характеристики потребляемой ей мощности, и на основе их анализа появляется материал для вычисления секретного ключа и используемых в смарт-карте протоколов и алгоритмов. Более детальное описание методики и технические детали можно прочитать на сайте, автор которого — тот же Кочер (www.cryptography.com/resources/whitepapers/DPA.html).

Так как методика анализа мощности смарт-карт опубликована сравнительно недавно, пока не изобретено практических решений по предотвращению таких атак. Те немногие методы, которые предложены для этой защиты, должны быть внедрены в смарт-карты. Самый перспективный метод, при котором в цепь электропитания смарт-карты включается диодно-конденсаторная схема, был предложен Ади Шамиром.

Атаки на отказ (сбой) программного протокола (имеется в виду не только протокол передачи, но и порядок выполнения программного кода) направлены на недоработки или ошибки чипа. Подобные атаки требуют детально проанализировать схемотехнику чипа и его программное обеспечение или долго и кропотливо изучать чип методом проб и ошибок, чтобы определить, как он реагирует на разные воздействия: быстрые или медленные тактовые частоты, колебания уровня электропитания и другие имитации сбоев окружающей среды.

Например, следующая технология может быть использована для изменения состояния контрольных устройств (датчиков на кристалле). Если использовать сигнал от часов или случайное значение из многопоточных операций для изменения внутренней тактовой частоты, то будет предотвращено предсказание времени выполнения команд. Кроме того, многие смарт-карты выпускаются с установленными в них контрольными датчиками, которые от-

ОСНОВНАЯ ПРОБЛЕМА СМАРТ-КАРТ — БЕЗЗАЩИТНОСТЬ ПЕРЕД ФИЗИЧЕСКОЙ АТАКОЙ, ПРИ КОТОРОЙ ЗЛОУМЫШЛЕННИК ИЗМЕНЯЕТ ВНЕШНОСТЬ С ПОМОЩЬЮ ПЛАСТИЧЕСКОЙ ХИРУРГИИ

ключают процессор, если изменяется внешняя тактовая частота, температура окружающей среды или уровень электропитания. Увы, эти датчики часто отключают, так как они довольно капризны в работе и сами становятся источником отказа чипа.

агрессивные атаки на смарт-карту

Агрессивная физическая атака на чип очень проста и может обеспечить доступ к его самым защищенным частям. Даже в Сети можно найти описание нескольких физических атак на смарт-карты. Атакующий может исследовать и проанализировать карточный чип в стандартной системе отладки, отсоединив процессор от платки. Разработка собственного отладочного комплекта не является чем-то сверхсложным. В книге Патрика Гелля «ПК и чип-карты» приводятся принципиальные схемы и тексты программ для подобных исследований смарт-карт. Кстати, для исследований магнитных карт у того же автора есть книга «Магнитные карты и ПК».

Острым ножом срезаешь пластмассу с чипа, пока не увидишь эпоксидную смолу, которой приклеен чип. Смолу удаляешь несколькими каплями концентрированной азотной кислоты (>98% HNO₃). Если предварительно подогреть смолу, процесс пойдет намного быстрее. Затем, полоская чип в ацетоне, добираться до кремниевой подложки самого чипа. Вынимаешь чип и помещаешь его в тестовую плату.

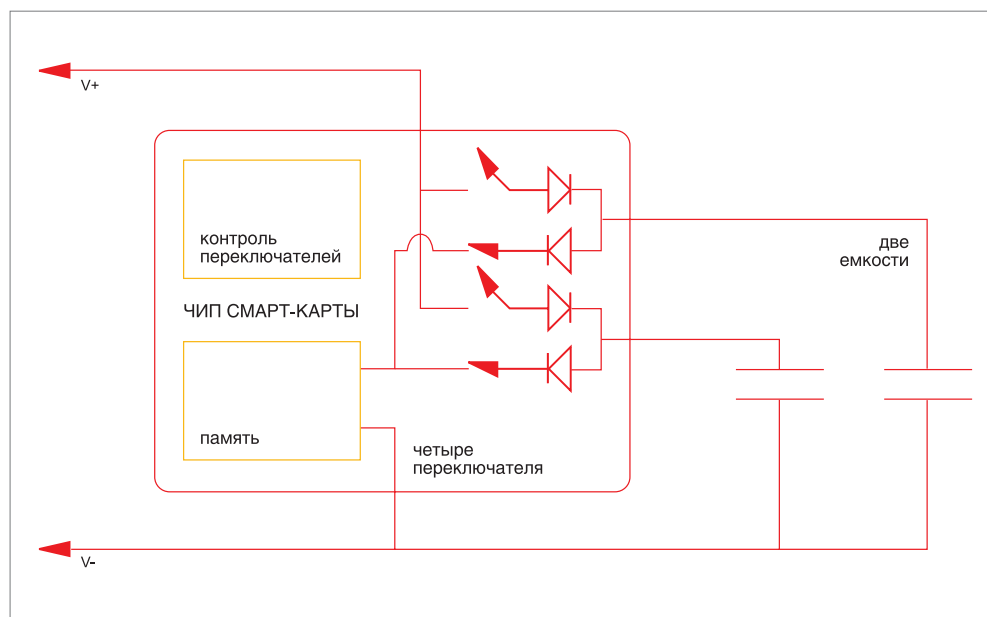
Теперь чип беззащитен, и его уже можно изучать. Два известных исследователя, Kuhn и Anderson, утверждают, что все нужные для манипуляций с чипом инструменты и материалы были куплены ими в аптеке за \$30. После описанной подготовки чип изучается с помощью микролазеров и тестеров с микрошупами для «влезания» внутрь схемы и считывания результата с контактов. Функциональные возможности карты могут быть изменены лазером, ультразвуком или направленным потоком ионов. Если кристалл будет извлечен, будет возможно изучить под обычным микроскопом и его. Плавкие предохранители на плате могут остаться на месте в процессе подготовки. Их можно обойти «закоротив» при помощи двух микрошупов. Такая «восстановленная» испытательная схема может быть использована для чтения памяти.

Те же Anderson и Kuhn опубликовали несколько других способов дешевых физических атак. Они утверждают, что смогли прочитать содержание памяти и даже изменить его, используя в качестве «редактора» направленный поток ионов. С помощью лазера своей установкой они смогли изменить состояние даже отдельных ячеек ПЗУ. Вот и серьезная опасность: существует атака на DES, при которой изменение нескольких бит приводит к дискредитации всей ключевой информации. Аналогично организуются атаки и на ППЗУ.

Но есть способ предотвратить такую атаку — установить емкостной датчик, который обнаруживает изменение объема или сопротивления среды. Второй способ — установить оптический датчик под непрозрачной фольгой, защищающей микросхему. Если защита сработает, то необратимо разрушит критическую информацию. Однако эти датчики недостаточно надежны, и поэтому распространены мало.

Фирма Philips предлагает свой способ защиты от физической атаки. Компания реклами-

ОДИН ИЗ ПРИЕМОВ ЗАЩИТЫ ОТ АГРЕССИВНОЙ АТАКИ — УСТАНОВКА ЕМКОСТНОГО ДАТЧИКА, КОТОРЫЙ ОБНАРУЖИВАЕТ ИЗМЕНЕНИЕ ОБЪЕМА ИЛИ СОПРОТИВЛЕНИЯ СРЕДЫ



рует технику так называемой логики клея (glue logic). На сайте Philips утверждается, что эта техника «перемешивает» логику чипа случайным образом. Похоже на технологию «визуального» шифрования, при которой блоки перемешаны настолько, что выяснить логику их соединения практически невозможно. Другой способ — защита памяти, при которой адрес и фактическое размещение данных никак не связаны. Однако такой подход работает только для динамических объектов, а следовательно, пригоден только для ОЗУ.

разделение полномочий Возможно, самый сложный вопрос в системах безопасности — проблема разделения полномочий, суть которой в том, что одна сторона контролирует часть функциональных возможностей смарт-карты и влияет на контроль функциональных возможностей другой стороны. Например, функциональные возможности смарт-карты потенциально разделены между вот этими сторонами:

- CARDHOLDER (ВЛАДЕЛЕЦ КАРТЫ).
- DATA OWNER (ВЛАДЕЛЕЦ ДАННЫХ).
- TERMINAL (POS-ТЕРМИНАЛ, АТМ И ВООБЩЕ ВСЕ, С ЧЕМ ВЗАИМОДЕЙСТВУЕТ КАРТА).
- CARD ISSUER (ВЫПУСТИВШИЙ КАРТУ В ОБРАЩЕНИЕ).
- CARD MANUFACTURER (ИЗГОТОВИТЕЛЬ КАРТЫ).
- CARD SOFTWARE DEVELOPER (РАЗРАБОТЧИК ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ).

И вот пример плачевного результата такого разделения. Жуликовский терминал списывает с карты одну сумму, а в чеке указывает другую либо сохраняет у себя частную информацию, например PIN. Такие нападения (имитатор банкомата) совершенно реальны.

При одном из способов предупредить атаки со стороны терминала на карту или, наоборот, со стороны кардхолдера на терминал процессинговый центр поэтапно контролирует процесс сделки и, если обнаруживается подозрительная деятельность, устанавливает флаг предупреждения. Большинство атак невозможны на стоящем отдельно компьютере, так как они в таком случае попадают во внимание единой системы безопасности. Совсем другая ситуация с системами на смарт-картах: функциональность (в том числе защиты) распределена между многими участниками.

Многофункциональные, а следовательно, самые универсальные карты потенциально уязвимы к нападениям именно из-за разделения полномочий безопасности по системам, которые они поддерживают. Множество приложений, которые поддерживает смарт-карта, требует солидного многообразия от средств аутентификации и безопасности в различных используемых системах. Ридер должен подтвердить подлинность (валидность) карты и cardholder'a, а карта, в свою очередь, валидность «считки» и аутентичности программного обеспечения. Кроме того, «считка» должна удостовериться в подлинности подключенных к ней периферийных устройств.

Один из главных недостатков смарт-карты заключается в том, что она не может самостоятельно связаться с «внешним миром» и вынуждена делать это через специальное оборудование (терминал). Шнайер и Шостак

СМАРТ-КАРТЫ ИСПОЛЬЗУЮТ ДАЖЕ ДЛЯ ОПЛАТЫ ПОКУПОК ЧЕРЕЗ ИНТЕРНЕТ

САМАЯ ПРОСТАЯ АТАКА — БЛОКИРОВАНИЕ ДОСТУПА К ОДНОМУ ИЗ КОНТАКТОВ НА КАРТЕ

КАРТЫ С РАЗДЕЛЕНИЕМ ПОЛНОМОЧИЙ БЕЗОПАСНОСТИ ПОТЕНЦИАЛЬНО УЯЗВИМЫ НАПАДЕНИЯМ

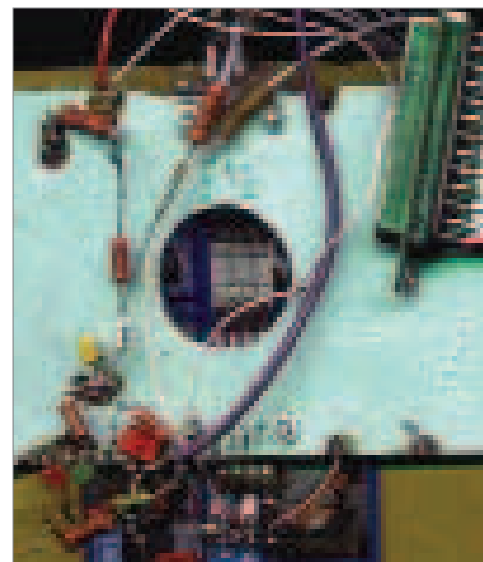
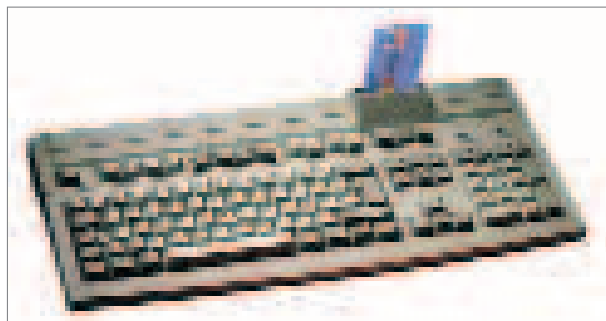
(Schneier and Shostack) рекомендуют объединить владельца карты и владельца данных в одно лицо. Часто cardholder и data owner и являются одним лицом, но карточные приложения не всегда принимают этот факт и разделяют доступ — это самый простой и дешевый способ защититься от определенного вида атак, которые являются чумой для многих систем, основанных на смарт-картах. Альтернативный и более дорогой способ уменьшить проблемы разделения полномочий — введение в карту устройства ввода данных и экрана.

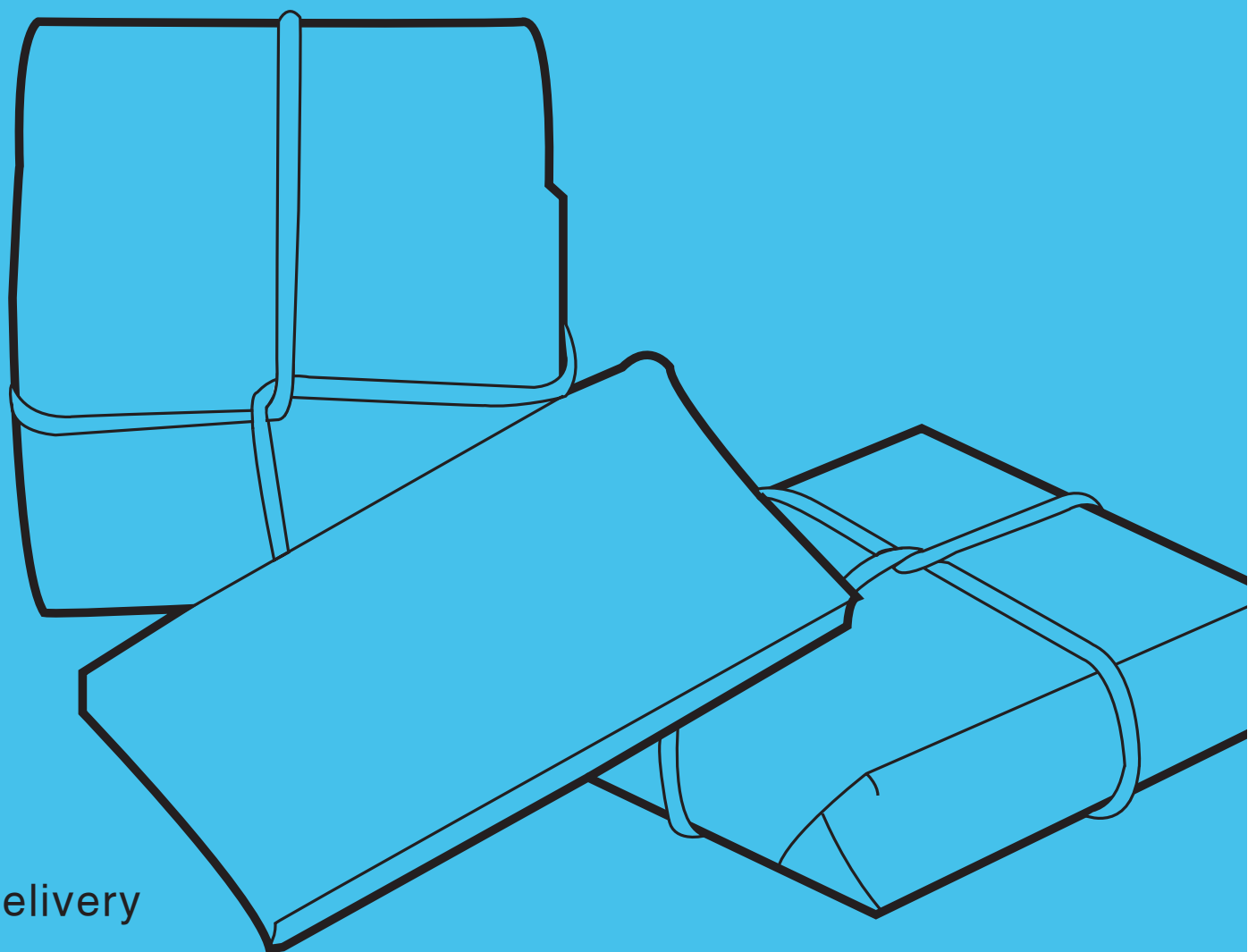
И, наконец, чтобы улучшить защиту, необходимо позволять независимым экспертам участвовать в разработке и тестировании подобных систем (так сделано в гражданской криптографии). Этот подход уже показал себя с лучшей стороны в повышении устойчивости защиты на многих системах. В проекте Mondex, например, система позволяет пользователям проверять некоторые параметры, независимые от торгового терминала. Методы защиты такого рода противостоят самым разным атакам: если используются «открытый код» (то есть исходные тексты и математические модели, доступные для анализа и обсуждения еще до их внедрения) и открытые ясные спецификации, то станет ли разработчик этих приложения осуществлять атаки?

закключение Если бы от меня потребовали назвать преимущество смарт-карт одним словом, то я сказал бы «удобство». Многофункциональные смарт-карты универсальны и удобны, но они наиболее уязвимы разным атакам. Основная проблема сейчас — это неэффективная защищенность смарт-карт перед дешевым способом физической атаки, при которой мошенник изменяет внешность обратившись к пластической хирургии.

Смарт-карты — не панацея от всех бед защиты данных, они всего лишь сочетание (уникальное сочетание — других способов не существует) дешевизны, малых размеров, портативности и повышающейся универсальности. Скорость вычислений и криптографические возможности карт повышаются с каждым годом. Если эта тенденция сохранится в дальнейшем, то смарт-карты найдут и займут такие прикладные ниши, о которых сейчас мы даже не можем предположить.

слева направо:
Карт-ридеры позволяют втыкать смарт-карты и в ноуты, и в клавиатуры
Примерно так выглядит трепанация чипа





special delivery

F.A.Q
ОБЗОР САЙТОВ

ЗАКАЗ ЖУРНАЛА В РЕДАКЦИИ

Бесплатные телефоны
по всем вопросам подписки
780-88-29 (по Москве),
8-800-200-3-999
(для регионов и абонентов МТС,
Билайн, Мегафон)

ВЫГОДА

Цена подписки на 20% ниже, чем в розничной продаже
Бонусы, призы и подарки для подписчиков
Доставка за счет редакции

ГАРАНТИЯ

Ты гарантированно получишь все номера журнала
Единая цена по всей России

СЕРВИС

Заказ удобно оплатить через любое отделение банка
Доставка осуществляется заказной бандеролью
или с курьером

СТОИМОСТЬ ЗАКАЗА НА ХАКЕР СПЕЦ+CD

900р

за 6 месяцев

1740р

за 12 месяцев



СТОИМОСТЬ ЗАКАЗА НА КОМПЛЕКТ ХАКЕР СПЕЦ+ХАКЕР+ЖЕЛЕЗО

2550р

за 6 месяцев

5040р

за 12 месяцев



ЗАКАЖИ ЖУРНАЛ В РЕДАКЦИИ И СЭКОНОМЬ ДЕНЬГИ

ПОДПИСНОЙ КУПОН

Прошу оформить подписку:

- на журнал Хакер Спец + CD
 на комплект Хакер Спец + Хакер + Железо

на месяцев
начиная с _____ 200_ г.

- Доставлять журнал по почте на домашний адрес
 Доставлять журнал курьером на адрес офиса (по г. Москве)
Подробнее о курьерской доставке читайте ниже*

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. _____

дата рожд. . . г.
день месяц год

АДРЕС ДОСТАВКИ:

индекс _____

область/край _____

город _____

улица _____

дом _____ корпус _____

квартира/офис _____

телефон (_____)
код

e-mail _____

сумма оплаты _____

* Курьерская доставка осуществляется только по Москве на адрес офиса. Для оформления доставки курьером укажите адрес и название фирмы в подписном купоне.

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО ММБ

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545

КПП - 772901001

Платательщик _____

Адрес (с индексом) _____

Назначение платежа

Сумма

Оплата за « _____ »

с _____ 200_ г.

Ф.И.О. _____
месяц

Подпись платателя _____

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО ММБ

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545

КПП - 772901001

Платательщик _____

Адрес (с индексом) _____

Назначение платежа

Сумма

Оплата за « _____ »

с _____ 200_ г.

Ф.И.О. _____
месяц

Подпись платателя _____

Кассир

Как оформить заказ

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном любым из перечисленных способов:

- по электронной почте: subscribe@glc.ru;
- по факсу: 780-88-24;
- по адресу: 119992, Москва, ул. Тимура Фрунзе, д. 11, стр. 44-45, ООО «Гейм Лэнд», отдел подписки.

ВНИМАНИЕ!

Подписка оформляется в день обработки купона и квитанции.

- купоны, отправленные по факсу или электронной почте, обрабатываются в течение 5 рабочих дней.
- купоны, отправленные почтой на адрес редакции обрабатываются в течение 20 дней.

Рекомендуем использовать электронную почту или факс.

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если произвести оплату в сентябре, то подписку можно оформить с ноября.

По всем вопросам, связанным с подпиской, звоните по бесплатным телефонам:

780-88-29 (для москвичей) и **8-800-200-3-999** (для регионов и абонентов МТС, БиЛайн, Мегафон).

Все вопросы по подписке можно присылать на адрес: info@glc.ru

Подписка для юридических лиц

Москва: ООО «Интер-Почта», тел.: 500-00-60, e-mail: inter-post@sovintel.ru

Регионы: ООО «Корпоративная почта», тел.: 953-92-02, e-mail: kpp@sovintel.ru

Для получения счета на оплату подписки нужно прислать заявку с названием журнала, периодом подписки, банковскими реквизитами, юридическим и почтовым адресом, телефоном и фамилией ответственного лица за подписку.

www.interpochta.ru

faq

ОТВЕТЫ НА НАИБОЛЕЕ ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

НАВЕРНОЕ, ПОСЛЕ ПРОЧТЕНИЯ СТАТЕЙ В ЭТОМ НОМЕРЕ У ТЕБЯ ВОЗНИКЛА МАССА ВОПРОСОВ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ ДЕНЕГ. В ЭТОЙ СТАТЬЕ Я ПОПЫТАЮСЬ ОТВЕТИТЬ НА НЕКОТОРЫЕ ИЗ НИХ | ДЕНИС КОЛИСНИЧЕНКО (DHSILABS@MAIL.RU)

WebMoney и «Яндекс.Деньги» сейчас являются самыми популярными системами в России, поэтому мы рассмотрим именно их. Начнем с «классики» — WebMoney.

webmoney

Я забыл свой WMID. Как восстановить его? Помню номер кошелька.

Попроси кого-нибудь, с кем ты имел дело в системе WebMoney, найти твой WMID с помощью Кеерер'а: перейти на закладку «Корреспонденты», нажать правую кнопку мыши и выбрать команду «Найти», в появившемся окне ввести номер кошелька. Ты можешь сделать это и сам, если зарегистрируешь новый WMID, но лучше попросить кого-то другого, чтобы не загружать систему «лишними» WMID.

Я не помню ни WMID, ни номера кошельков.

А твой ли это WMID? Ну ладно, это лечится. Попроси кого-нибудь, с кем ты имел дело в WebMoney, сообщить твои реквизиты. Связаться с таким человеком всегда можно — есть e-mail и электронная почта.

Если ты хочешь, чтобы никто не узнал о твоём склерозе, то данную информацию ищи в реестре Windows — HKEY_CURRENT_USER\Software\WebMoney\Options. Там ты найдешь раздел с номером твоего WMID. Ну а если причина твоего склероза — переустановка Windows, тогда отправь файл с ключом (он должен быть, ищи *.kvm-файл) и пароль по адресу support@webmoney.ru. Вся эта процедура обойдется в один WMZ — не так уж и много.

Я забыл свой пароль.

Функции отправки пароля по e-mail нет. Система электронных платежей — это не

какой-нибудь форум, все-таки разработчики WebMoney прежде всего заботятся о твоей безопасности. Ты должен написать письмо (прикрепив к нему файл с ключом (*.kvm) по адресу support@webmoney.ru и указать в нем следующую информацию:

- ТВОЙ WMID;
- ВАРИАНТЫ ПАРОЛЯ — КАКИМ ОН МОГ БЫТЬ.

Я забыл все.

А не пытаешься ли ты получить доступ к чужому WMID? Нет? Просто слетела вся информация на винчестере, вместе с файлом ключей, WMID, номерами кошельков...

Восстановить твой кошелек можно, если ты являешься аттестованным участником, то есть у тебя есть свой аттестат — только так можно установить, что ты — тот, за кого выдаешь себя. Если же аттестата нет, увы. Если же ты аттестованный участник, по вопросу восстановления можешь обратиться по адресу certsrv@webmoney.ru. Учти, что тебе нужно будет явиться в представительство WebMoney или отправить нотариально заверенное заявление о восстановлении. Само восстановление стоит 3 WMZ, если у тебя персональный аттестат, или 5 WMZ, если у тебя аттестат доверия.

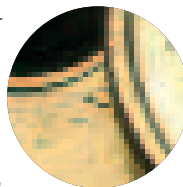
Как видишь, восстановление стоит недорого, но головная боль будет — и твоя, и представителей системы, поэтому сделай резервную копию ключа и всех данных (WMID, аттестата, номеров кошельков) и запиши ее на CD-R, который желательно спрятать куда-нибудь подальше от чужих глаз и рук. Если на твоём кошельке были одни нули, лучше не пытаться восстанавливать его. Просто заведи себе новый и сообщи всем, кто должен перевести тебе деньги, свой новый номер кошелька.

Я хочу совершить покупку в интернет-магазине, который принимает средства только по WebMoney. Не вижу необходимости регистрироваться в системе, потому что после этой покупки я не собираюсь больше пользоваться системой. Что мне делать?

Ты можешь попросить у интернет-магазина реквизиты (счет) для оплаты через банк или почтовое отделение. Помни, что в случае с банком твои деньги будут зачислены через один-два дня, а в случае с почтой — на следующий день. Можно также обратиться к обменному пункту WebMoney, если такой есть в твоём городе. Ты можешь договориться с работниками обменника о том, чтобы они купили тебе этот товар (перечислили деньги на нужный кошелек), а потом расплатиться с ними наличными. Список электронных обменников ты найдешь на www.webmoney.ru.

Участник не сообщил мне свои данные, а мне бы хотелось узнать о нём больше.

Ты, как и остальные участники, можешь не сообщать системе данные о себе (фамилию, адрес и т.д.), поскольку WebMoney является анонимной системой и



в ней тебя представляет только WMID. Но если ты просто заинтересовался, с кем имеешь дело, особых трудностей не возникнет. В строке адреса браузера набираем следующий адрес:

<https://certsrv.webmoney.ru/certview.asp?wmid=xxxxx> — это

WMID интересного тебе участника. Ты получишь ту информацию о пользователе, которую он сам предоставил системе. Поскольку система анонимна, эта информация может оказаться неправдивой.

Однако если у участника есть аттестат, то можно доверять информации. Если же в поле вместо значения стоит n/a, значит, пользователь запретил данное поле для показа. На практике обычно происходит следующее. Пользователь хочет сохранить анонимность, поэтому:

1 У НЕГО НЕТ АТТЕСТАТА, И ОН НЕ УКАЗЫВАЕТ ПРАВДИВУЮ ИНФОРМАЦИЮ О СЕБЕ.

2 У ПОЛЬЗОВАТЕЛЯ ЕСТЬ АТТЕСТАТ, НО ОН ЗАКРЫЛ ВСЕ ПОЛЯ — ТЫ НЕ СМОЖЕШЬ ПРОСМОТРЕТЬ ИХ.

Какая версия удобнее: Web Money Keeper Classic или Light?

«Классика» выполнена в виде обычного Windows-приложения, а Light-версия — это всего лишь web-интерфейс для доступа к системе. «Классическая» версия удобнее, чем «облегченная». Ты можешь использовать только одну версию: или Light, или Classic. Не нужно думать, что дома ты можешь использовать Classic-версию, а вне дома — Light. Это не почтовая система, где дома тебе The Bat, а в интернет-кафе — Internet Explorer. Выбирай сам: Light мобильна, а Classic — удобна. Правда, есть еще одно НО. Если у тебя Linux, то тебе достанется только Light-версия, так как Classic-версия для Linux пока нет.

Есть ли Classic-версия для Linux?

К сожалению, пока версии WM Keeper для Linux нет. Если у тебя установлен Linux, нужно или использовать Light-версию, или установить эмулятор Windows (я рекомендую VMWare) и попробовать использовать Keeper через него. Теоретически все должно работать, правда, я не проверял: руки не дошли.

Как часто нужно менять пароль и стоит ли вообще делать это?

Менять пароль из соображений безопасности рекомендуется один раз в месяц. Чем чаще, тем лучше, но только не перестарайся, иначе запутаешься. При смене пароля выбирай сложный для подбора, но в то же время легко запоминающийся пароль, например audiA41320kg. Запомнить пароль очень легко. Предположим, твой любимый автомобиль — Audi модели A4, и он весит 1320 кг (точно не знаю, но что-то вро-

де того). Запомнить очень легко, а подобрать — сложно. При выборе пароля старайся использовать разные регистры символов, чтобы в пароле были и заглавные, и строчные буквы. Для смены пароля выбери пункт меню «Настройки» > «Программы». На вкладке «Безопасность» нажми «Сменить пароль». В появившемся окне введи новый пароль. Обрати внимание на дополнительные параметры этой вкладки. Здесь ты также можешь изменить ключи — это рекомендуется, если ты подозреваешь, что кто-то украл твои ключи. Хорошо бы также увеличить размер ключа до 10 Мб, некоторые программы позволяют передать твой ключ на компьютер злоумышленника. Передать 10 Мб по нашим каналам связи сложнее, чем 1 Мб. Хотя и это не панацея...

А это что такое? Я не могу создать кошелек! Появляется пустое окно — без сообщений и кнопок. Если я его закрываю, кошелек не создается. Что делать?

В некоторых версиях Keeper'a действительно есть такая проблема. Поможет апгрейд IE до версии 6.0. Если обновлять IE не хочется, просто нажми <Enter>, когда появится это окно.

Можно ли перевести деньги с кошелька на пластиковую карточку?

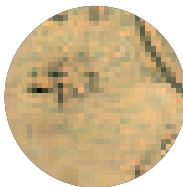
Да, можно. По сути, это обычный банковский перевод. Реквизиты для перевода ты можешь узнать в банке, в котором открыл счет. Обрати внимание: номер карточки и номер счета — это разные вещи, поэтому необязательно, чтобы номера совпадали. Перед переводом обязательно уточни все в банке, иначе отправишь деньги непонятно куда.

Я не могу подключиться к системе. Keeper сообщает: «Невозможно подключиться к центру сертификации...»

Если с интернетом все в порядке, то причина в прокси-сервере. Если прокси установлен в локальной сети, попроси администратора открыть порт 2802 (это порт WebMoney) для IP-адресов 212.158.173.75, 212.158.173.76, 212.158.173.6, 212.158.173.7, 212.158.173.46, 195.133.120.6, 195.133.120.7 (это IP-адреса серверов WebMoney). Если же прокси установлен у провайдера, то нужно сделать то же самое (попросить администратора открыть указанный порт для указанных адресов). Правда, это будет сложнее, но, по идее, провайдер не должен отказать тебе. В случае отказа или смени провайдера, или установи программку HTTPPort, которая позволяет «обойти» прокси провайдера.

При попытке отправить деньги получаю сообщение: «Вы не авторизованы корреспондентом для выполнения данной операции».

Чтобы ты мог отправить деньги другому участнику системы, ты должен быть авторизован им. Вообще авторизация



не обязательна, и она не используется по умолчанию. Если ты увидел это сообщение, значит, авторизации требует сам участник. Чтобы ты мог отправить ему деньги, попроси его сделать одно из следующих действий:

- ВЫПОЛНИТЬ КОМАНДУ МЕНЮ «МЕНЮ» > «НАСТРОЙКИ» > «ПРОГРАММЫ», ПОТОМ ПЕРЕЙТИ НА ЗАКЛАДКУ «ОГРАНИЧЕНИЯ» И ВКЛЮЧИТЬ ОПЦИЮ «ПЛАТЕЖИ»;
- ОТПРАВИТЬ ЕМУ ЗАПРОС НА АВТОРИЗАЦИЮ (КОМАНДА «МЕНЮ» > «ЗАПРОС НА АВТОРИЗАЦИЮ») И ПОПРОСИТЬ ПОЛУЧАТЕЛЯ АВТОРИЗОВАТЬ ТЕБЯ.

Запускаю Кеерг и вижу «картину»: «Возможно, файлы WebMoney Кеерг Classic были повреждены или модифицированы! Настоятельно рекомендуется переустановить программу. Скачать файл установки WebMoney Кеерг Classic прямо сейчас?»

Переустанови Кеерг. Данная ошибка появляется, если ты хочешь установить Кеерг в каталог, название которого содержит русские буквы.

«ЯНДЕКС.ДЕНЬГИ»

Web-интерфейс или «Интернет.Кошелек»? Что выбрать?

Выбирай сам. Web-интерфейс — это что-то наподобие Light-версии WebMoney, он предельно прост и его можно использовать в любой операционной системе. «Интернет.Кошелек» гибче в настройке, у него привычный интерфейс Windows-программы. Если сравнивать эти две версии по степени защищенности, то разработчики системы уверяют, что web-интерфейс так же безопасен, как и «Интернет.Кошелек».

У тебя Linux? Тогда используй web-интерфейс. Если он тебе не нравится, установи эмулятор Windows, а в нем — программу «Интернет.Кошелек».

«Слетела» вся информация на винте! Что делать?

Если у тебя не осталось резервной копии «Интернет.Кошелек» и ты не указывал при регистрации свои паспортные данные, никто не сможет помочь тебе. Если же ты указал правильные паспортные данные, система сможет вернуть тебе твои деньги. Поэтому подумай, что для тебя важнее: анонимность или возможность вернуть свои деньги в случае ЧП. На сайте money.yandex.ru ты узнаешь, что нужно сделать, чтобы вернуть свои деньги.

Ты еще не сделал резервную копию? Сделать сейчас же, желательно на компакт-диске, чтобы потом не обращаться в компанию за помощью.

Как восстановить кошелек из резервной копии?

Установи «Интернет.Кошелек» заново, но не запускай его. В твоей резервной копии будут каталоги Data и DB. Замени соответствующие каталоги на жест-

ком диске каталогами из резервной копии. Далее запусти «Интернет.Кошелек» и обязательно выполни синхронизацию данных — программа сама предложит сделать это.

Может ли у меня быть несколько кошельков?

Да, на один компьютер (или на разные) ты можешь установить несколько «Интернет.Кошельков», при этом каждый из них будет связан с разным счетом в системе (в процессинговом центре).

Что означает сообщение «Карточка заблокирована?»

Если при пополнении счета предоплаченной карточкой ты видишь это сообщение, значит, карточка еще не отмечена как проданная. Попробуй повторить попытку через несколько часов. Если не помогает, обратись в службу поддержки.

Где я могу пополнить свой счет?

То, где ты живешь, не играет роли: банки и почта есть везде, в любом городе. Пойди в любой банк или в отделение почты и переведи деньги на свой счет (или счет другого человека, если ты должен ему деньги, например за товар или программу). На сайте money.yandex.ru ты узнаешь все необходимые для этого реквизиты.

Сколько стоит одна операция в системе?

За каждую операцию с получателя взимается 0,5%. При выводе денег из системы взимается комиссия в размере 3% + 10 рублей при безналичном банковском переводе, плюс комиссия агента — банка или почты. Дорого, правда? Что же поделаешь?

Можно ли перевести деньги на пластиковую карточку?

С любой карточкой связан определенный расчетный счет. Если ты знаешь номер этого счета (это не номер карточки!) и остальные реквизиты банка, то можешь просто выполнить банковский перевод, и деньги будут зачислены на карточку. Фактически, перевод на карточку — это обычный банковский перевод.

Может ли юридическое лицо работать с системой «Яндекс.Деньги»?

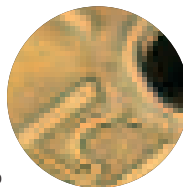
Да, может, но для этого нужно заключить специальный договор. Подробности ищи на сайте системы.

Начисляются ли проценты за хранение средств в системе?

Нет, проценты не начисляются. Если ты заинтересован в сбережении своих средств, открой депозитный счет в одном из банков.

Обязательно оставлять информацию о себе?

Система «Яндекс.Деньги» анонимна. Не указывать правдивую информацию о себе — это твое право.



Побывали в далеких странах?
Накопилось много интересных
фотографий?

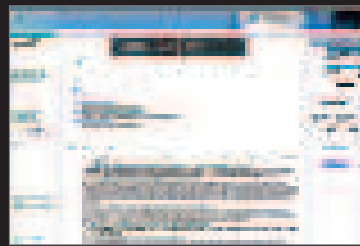


Создайте свой цифровой фотоархив на
<http://foto.mail.ru/> и покажите друзьям!

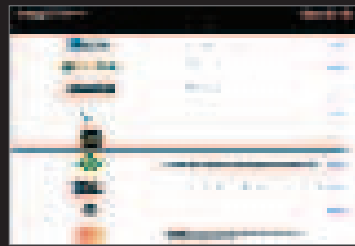
1. Доступ из любой точки мира
2. Удобная система альбомов
3. Редактирование фотографий
4. Возможность ограничения доступа только для друзей
5. Рейтинги лучших фотографий
6. Творческие конкурсы с призами

ФОТО@MAIL.RU[®]

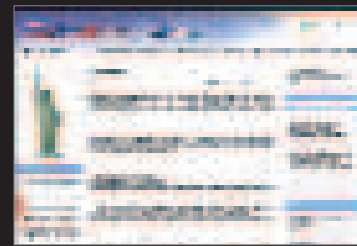
Ваш личный цифровой фотоархив!



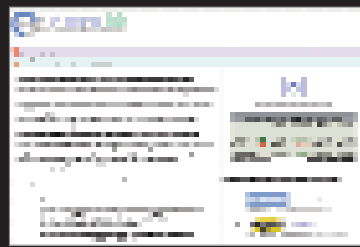
1 www.wfin.ru



2 www.emoney.ru/esystem



3 www.ruamerica.com



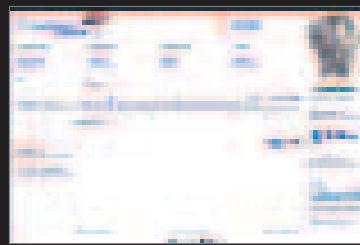
4 www.e-mex.biz



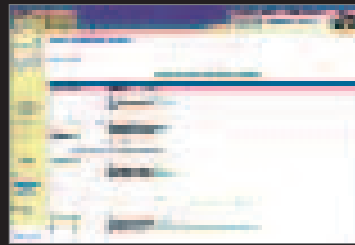
5 www.yourpay.ru



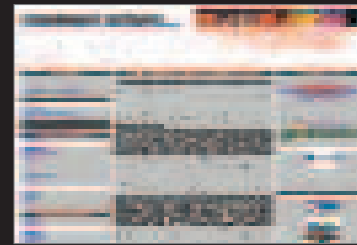
6 www.quickpay.ru



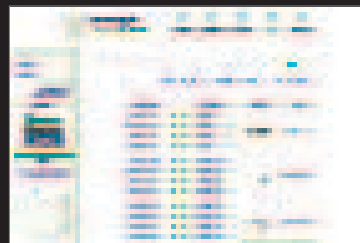
7 www.expressoplata.ru



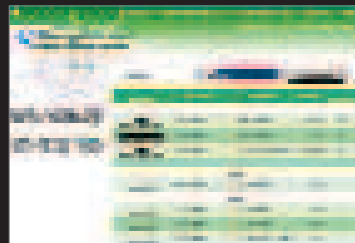
8 www.goldcity.ru



9 www.dsg.front.ru



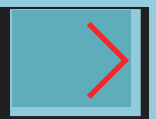
10 www.changemoney.ru



11 www.enavigator.ru



12 www.cnews.ru



обзор сайтов

САМЫЕ ВКУСНЫЕ САЙТЫ ПРО E-MONEY

МНОГООБРАЗИЕ ПЛАТЕЖНЫХ СИСТЕМ И РЕСУРСОВ, ПОСВЯЩЕННЫХ E-MONEY, НАСТОЛЬКО ВЕЛИКО, ЧТО РАЗОБРАТЬСЯ В НИХ БЕЗ ГИДА НЕВОЗМОЖНО, ПОЭТОМУ МЫ И ПРЕДЛАГАЕМ ЭКСПРЕСС-ПУТЕВОДИТЕЛЬ | АШОТ ОГАНЕСЯН (777@real.xakep.ru)



1 www.wfin.ru Один из лучших сайтов рунета, посвященный виртуальным деньгам в самом полном понимании этого термина и электронным платежным системам в частности. На ресурсе ты найдешь актуальные новости ключевых игроков этого рынка, описание большинства популярных систем, подробные инструкции по использованию той или иной интернет-системы. Особенно вкусный раздел, в котором множество материалов посвящено теме мошенничества с помощью электронных платежных систем и способам того, как не стать жертвой злоумышленников. Помимо интернет-денег, ты найдешь на ресурсе очень много информации по кредитным картам, вопросам их использования и проч. Очень любопытен и нетрадиционен раздел «Галерея дизайна банковских карт» — фотографии платежных карт массы крупных банков России.

Кроме того, здесь множество нормативно-справочных документов, регламентирующих операции с цифровой наличностью, комментарии официальных лиц относительно спорных положений. Можно также скачать глоссарий терминов, используемых в платежных и расчетных системах. Имеются специальные разделы, посвященные конкретным картам: Visa International cards, MasterCard International cards и American Express cards. Однозначно, один из самых полных и информативных ресурсов рунета, посвященный виртуальным платежам. Настоятельно рекомендуется к постоянному пользованию.

2 www.emoney.ru/esystem Еще один довольно неплохой ресурс по теме нашего номера. Смущает только одно обстоятельство: главная страница сайта не грузится по загадочной причине и делает это, по всей видимости, достаточно давно :). Впрочем, если постараться, можно, например зайдя по ссылке www.emoney.ru/esystem, получить весьма интересную подборку по иностранным платежным системам и их особенностям. Довольно редкая информация на русском языке, собирать ее по разным источникам не очень удобно. Вердикт таков: неплохой краткий справочник по иностранным платежным системам.

3 www.ruamerica.com RuAmerica — весьма и весьма полезный сервис для определенной группы пользователей, предоставляемый одноименной компанией, которая была организована летом 2004 года и являлась дочерней компанией Western Express/Paycard2000.com. В начале 2005 года компания обрела самостоятельность. RuAmerica предлагает свою помощь в приобретении товаров в интернете, а также на аукционах. Кроме того,

оказываются услуги по выставлению лотов на продажу на крупнейшем в мире интернет-аукционе eBay. По заявлению самой RuAmerica, компания связывает продавца и покупателя на любых стадиях их отношений — от получения заказа, контакта с продавцом до доставки товара заказчику. Кроме того, возможна услуга по получению адреса в США, который может быть использован для получения чеков от спонсоров. Реализовано также обналечение чеков, вывод средств со счетов Webmoney и E-gold, получение Tax-ID.

4 www.e-mex.biz Довольно нетрадиционный ресурс — площадка для автоматического гарантированного обмена различных электронных валют между участниками соответствующих систем. По сути, это электронная биржа для обмена валют по взаимовыгодному курсу. Алгоритм взаимодействия прост: участник осуществляет постановку заявки в очередь (перечень заявок) на обмен одной электронной валюты на другую по устраивающему его курсу. Если другой участник осуществляет заявку на противоположный обмен электронных валют по устраивающему обоим участникам курсу, происходит сделка — автоматический обмен средств между счетами участников в системе, по устраивающему обоим участникам курсу и в объеме произведенных заявок. За предоставление услуг такого рода площадка берет комиссию в размере 0,1% от суммы сделки. Поддерживаемые системы — WebMoney и E-Gold.

5 www.yourpay.ru Еще один очень полезный сервис — обменный центр между различными платежными системами. Список поддерживаемых систем весьма велик: PayPal, FirePay Neteller, e-Bullion, MoneyOrder, WesternUnion, MoneyGrem, ACH, wire transfer и др. Интересна услуга «океширования» на адрес в США от процессингов, биллингов, мерчантов и спонсоров.

Истинные геймеры оценят возможность пополнения че-

Обмениваемая система	
PayPal->WebMoney	15%
PayPal->Приват24 (USD)	13% (+ ком. системы)
PayPal->PayCash (UAH)	13%
FirePay->WebMoney	20%
e-Bullion->WebMoney	15%
Neteller->WebMoney	20%
PayCash->WebMoney	10%
MoneyOrder->WebMoney	10%
Check->WebMoney	10%
Wire Transfer->WebMoney	5%
Приват24 (USD)->Anyone	4% (+ ком. системы)
WebMoney->PayPal	4%
WebMoney->FirePay	0%
WebMoney->e-Bullion	5%
WebMoney->Neteller	5%
WebMoney->check	2%
WebMoney->Wire Transfer	1% (+ \$30)
WebMoney->Money Order	2%
WebMoney->Paycash (UAH)	1%
WebMoney->Приват24 (USD)	2% (+ ком. системы)
PayCash (UAH)->Anyone	1%

рез систему игровых аккаунтов во многих онлайн-играх, таких как SWG, EVE-Online и др. Аналогично описанному выше ресурсу RuAmerica.com, через Yourpay можно купить нужную тебе вещь на любом аукционе (eBay, Yahoo, Music Stock и др.), затем проделать все вплоть до доставки. Для многих честных (!) пользователей ПК окажется полезным приобретение программного обеспечения, которое невозможно достать, находясь в России. Здесь Yourpay также может обеспечить полный цикл покупки.

6 **www.quickpay.ru** Не очень известная и весьма небольшая платежная система, которая, тем не менее, очень удобна для микроплатежей. Например, с помощью Quickpay легко пополнить баланс телефона всех российских операторов сотовой связи, в том числе региональных, таких как «Алтайсвязь», «Юнисел» и др. Именно возможность проведения платежей региональным операторам сотовой связи и является отличительной чертой данной платежной системы. Очень удобен также сервис приема платежей с сотового телефона с помощью WAP или GPRS.

7 **www.expressoplata.ru** Один из самых удобных и многофункциональных центров приема электронных платежей в рунете. Здесь принимаются платежи за мобильную связь, доступ в интернет, спутниковое телевидение, хостинг, можно приобрести еврокреды для пополнения своего счета в игре **combats.ru** или оплатить их через WebMoney. Интересный сервис — пополнение счетов в платных MP3-архивах. Просто и со вкусом. Поддерживаемые системы — WebMoney и «Яндекс.Деньги». Продаются также пин-коды карт предварительной оплаты услуг сотовой связи многих операторов, а также карты доступа в интернет и проч. А вот обналичивание средств в системе неудобно. Во-первых, есть существенные ограничения на суммы: для сумм в рублях не более 12 000, в долларах — не более 500, в евро — не более 400. Во-вторых, взимается весьма внушительная комиссия в 10% от обналичиваемой суммы.

8 **www.goldcity.ru** Все очень просто, но нестандартно — WebMoney- и E-Gold-вклады под проценты. На ресурсе ты найдешь множество полезной информации по инвестированию в виртуальном мире. Но самое полезное — своеобразные рейтинги надежности инвестиционных фондов, разделенных по трем степеням: проверенные платежные фонды, новые и проверяемые платежные фонды и, наконец, проблемные фонды. Подробную информацию по инвестиционным фондам смотри в табличке*.

9 **www.dsg.front.ru** Очень интересный и полезный ресурс, посвященный электронным деньгам. Масса полезной информации, ссылки, статьи, новости, особенности конкретных платежных систем и многое другое. Ресурс очень удобно разделен по конкретным системам: WebMoney, PayCash, «Яндекс.Деньги», «Рапида», E-Port, «Кредит.Пилот», RuPay, CyberPlat, Assist, PayPalEAccess — множество рассмотренных систем не может не радовать. Присутствуют и такие экзотические на российском рынке системы, как PayAce и GreenZap. Отдельный раздел — «Платежные системы EN». Как можно догадаться по его названию, он посвящен иностранным платежным системам, таким как E-Gold, StormPay, PayPal, Moneybookers. Однозначно, один из лучших ресурсов рунета по количеству представленной информации о различных системах. К недостаткам можно отнести не очень дружелюбный дизайн: довольно некомфортно читать текст, написанный белым шрифтом по темно-зеленому фону. Тем не менее, ресурс настоятельно рекомендуется к ознакомлению.

10 **www.changemoney.ru** Как нетрудно догадаться по названию, Changemoney — очередной обменный центр цифровой наличности. Как гласит сам ресурс, «ChangeMoney.ru — это сервис, который позволяет в автоматическом режиме (всего за несколько секунд) обменять одну электронную валюту на другую». Обмен действительно крайне прост и очень быстр. Тарифы достаточно стандартные, впрочем, как и процедуры обмена. Сайт честно предупреждает, что в случае перевода денег на «не тот» коше-

*таблица рейтингов инвестиционных фондов

проверенные платящие фонды	
Swiftinvest	ПРОЦЕНТЫ — 4% — 5% В ДЕНЬ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 1\$ ПАРТНЕРСКАЯ ПРОГРАММА — 5% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 14.03.2005 СТАТУС — ОЖИДАНИЕ
Oceanic Financial	ПРОЦЕНТЫ — 1.7% В ДЕНЬ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 10\$ ПАРТНЕРСКАЯ ПРОГРАММА — 10% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 30.10.2004 СТАТУС — ПЛАТИТ ЕСТЬ ВОЗМОЖНОСТЬ РЕИНВЕСТИЦИИ
SmartVIP	ПРОЦЕНТЫ — 7% В ДЕНЬ, 170% ЗА 15 ДНЕЙ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 1\$ ПАРТНЕРСКАЯ ПРОГРАММА — 5% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 16.07.2005 СТАТУС — ОЖИДАНИЕ
новые и проверяемые фонды	
IDann Ltd.	ПРОЦЕНТЫ — 3% В ДЕНЬ, 23% В НЕДЕЛЮ, 48% ЗА ДВЕ НЕДЕЛИ, 100% В МЕСЯЦ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 10\$ ПАРТНЕРСКАЯ ПРОГРАММА — ДО 5% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD, E-BULLION, PECUNIX, EESECURRENCY, БАНКОВСКИЕ ПЕРЕВОДЫ ДАТА ОТКРЫТИЯ ПРОЕКТА — 24.08.2005 СТАТУС — ПЛАТИТ
Paxmix	ПРОЦЕНТЫ — 1.98% — 2.48% В ДЕНЬ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 5\$ ПАРТНЕРСКАЯ ПРОГРАММА — 10% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 22.08.2005 СТАТУС — ОЖИДАНИЕ
Golddaze	ПРОЦЕНТЫ — 1.2% В ДЕНЬ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 10\$ ПАРТНЕРСКАЯ ПРОГРАММА — 3% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 10.02.2005 СТАТУС — ПЛАТИТ
Reinvest Group	ПРОЦЕНТЫ — 1.1% — 3.1% В ДЕНЬ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 10\$ ПАРТНЕРСКАЯ ПРОГРАММА — 10% ОТ ДНЕВНОГО ДОХОДА ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD, EBULLION, INTGOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 31.07.2005 СТАТУС — ОЖИДАНИЕ
проблемные фонды	
E-moneyinvest	ПРОЦЕНТЫ — 1% — 3% В ДЕНЬ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 5\$ ПАРТНЕРСКАЯ ПРОГРАММА — 4% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 20.04.05 СТАТУС — ПРОБЛЕМЫ ОТ 5\$ — 2% В ДЕНЬ НА 100 ДНЕЙ, ОТ 10\$ — 3% В ДЕНЬ НА 60 ДНЕЙ, ОТ 50\$ — 6% В ДЕНЬ НА 40 ДНЕЙ, ОТ 100\$ — 10% В ДЕНЬ НА 20 ДНЕЙ ПРОЦЕНТЫ НАЧИСЛЯЮТСЯ ТОЛЬКО В РАБОЧИЕ ДНИ
Smith & Jacoby	ПРОЦЕНТЫ — 1.5% — 1.7% В ДЕНЬ, 12% — 12.6% В НЕДЕЛЮ, 200% ЗА 100 ДНЕЙ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 10\$ ПАРТНЕРСКАЯ ПРОГРАММА — 5% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 02.05.2005 СТАТУС — ПРОБЛЕМЫ
Grand hyp	ПРОЦЕНТЫ — 10% — 20% В ДЕНЬ, 125% — 200% В НЕДЕЛЮ, 170% — 350% ЗА ДВЕ НЕДЕЛИ, 330% — 680% В МЕСЯЦ МИНИМАЛЬНАЯ СУММА ВКЛАДА — 1\$ ПАРТНЕРСКАЯ ПРОГРАММА — 3% — 7% ПЛАТЕЖНЫЕ СИСТЕМЫ — E-GOLD ДАТА ОТКРЫТИЯ ПРОЕКТА — 23.06.2005 СТАТУС — ПРОБЛЕМЫ

лек тебе уже никто не поможет и кровные средства не будут возвращены. Жаль только, что обмен производится лишь между двумя платежными системами: WebMoney и E-Gold.

11 **www.enavigator.ru** Полноценный вариант предыдущего ресурса, однако здесь обмен цифровой наличностью возможен не только с WebMoney и E-Gold, но и с «Яндекс.Деньги» и еще целым рядом электронных платежных систем. Изюминка ресурса в том, что это не обменник, а отличный информер по многим другим обменным пунктам цифровой наличности с указанием их актуальных тарифов. Очень быстро, информативно и удобно. Отрадно также, что услуги e-navigator'a абсолютно бесплатны. Может послужить неким пособием для начинающего трейдера на рынке цифровой наличности (а почему нет? :)). Есть любители такой экзотики?

12 **www.cnews.ru** Крупнейший интернет-портал рунета по информационным технологиям, посещаемость достигает 75-80 тысяч уникальных (!) пользователей в день, а количество показов на главной странице превышает 200 000 в день. Разумеется, cnews.ru не может обделить вниманием тему электронной коммерции и цифровой наличности. Именно на этом ресурсе достаточно регулярно печатаются статьи, посвященные бизнесу основных игроков рынка электронных платежных систем страны: их доходы, обороты, структура выручки, сервисы и проч. Также на ресурсе имеются интервью с представителями электронных платежных систем.

ВЫБИРАЕМ ДОМАШНИЙ КИНОТЕАТР

Тесты техники, советы по выбору и установке домашнего кинотеатра - ЖК-телевизоры, AV-ресиверы, DVD-плееры, акустика и многое другое.

СМОТРИ СЛУШАЙ ЧУВСТВУЙ 12 (16) ДЕКАБРЬ 2005

ВЫБИРАЕМ ДОМАШНИЙ КИНОТЕАТР

DVD ЭКСПЕРТ

10 ЭКСПЕРТОВ ПРОВЕЛИ БОЛЕЕ 400 ЧАСОВ В ЛАБОРАТОРИИ, ЧТОБЫ ПРЕДОСТАВИТЬ ВАМ ТЕСТЫ 7 ПРОИГРЫВАТЕЛЕЙ ГРАМПЛАСТИНОК, 6 DVD-СИСТЕМ, 5 ВИДЕОПРОЕКТОРОВ, 4 ПАР АКУСТИКИ, 4 ЖК-ТЕЛЕВИЗОРОВ, 3 DVD-ВИДЕОКАМЕР, 2 AV-РЕСИВЕРОВ И 2 DVD-ПЛЕЕРОВ



Хью Джекмен, Кейт Бекинсейл, Ричард Роксбург в фильме Стивена Соммерса **ВАН ХЕЛЬСИНГ** (2004).*

*100% гарантия широкоэкранного анаморфного изображения; звуковые дорожки DD5.1. DVD-приложения к журналу соответствуют уровню качества ЛУЧШИХ мировых изданий!



НЕ ОГРАНИЧИВАЙ СЕБЯ

Играй
просто!
GamePost

ПОЛУЧИ
МАКСИМУМ
УДОВОЛЬСТВИЯ

ИСПОЛЬЗУЯ ДОПОЛНИТЕЛЬНЫЕ АКСЕССУАРЫ



Монитор
Shuttle XP17SG

\$675.99



Наушники
Sennheiser RS 110-8

\$79.99



Колонки
M-Audio Studiophile
LX4 2.1 System

\$339.99



Шлем
i-O Display Systems
i-glasses PC

\$1099.99



Копнус
Shuttle SB83G5C

\$485.99



Pinnacle Systems
Studio 9 Plus RUS

\$99.99

* Большой выбор
PC аксессуаров

* Товары от
самых лучших
производителей

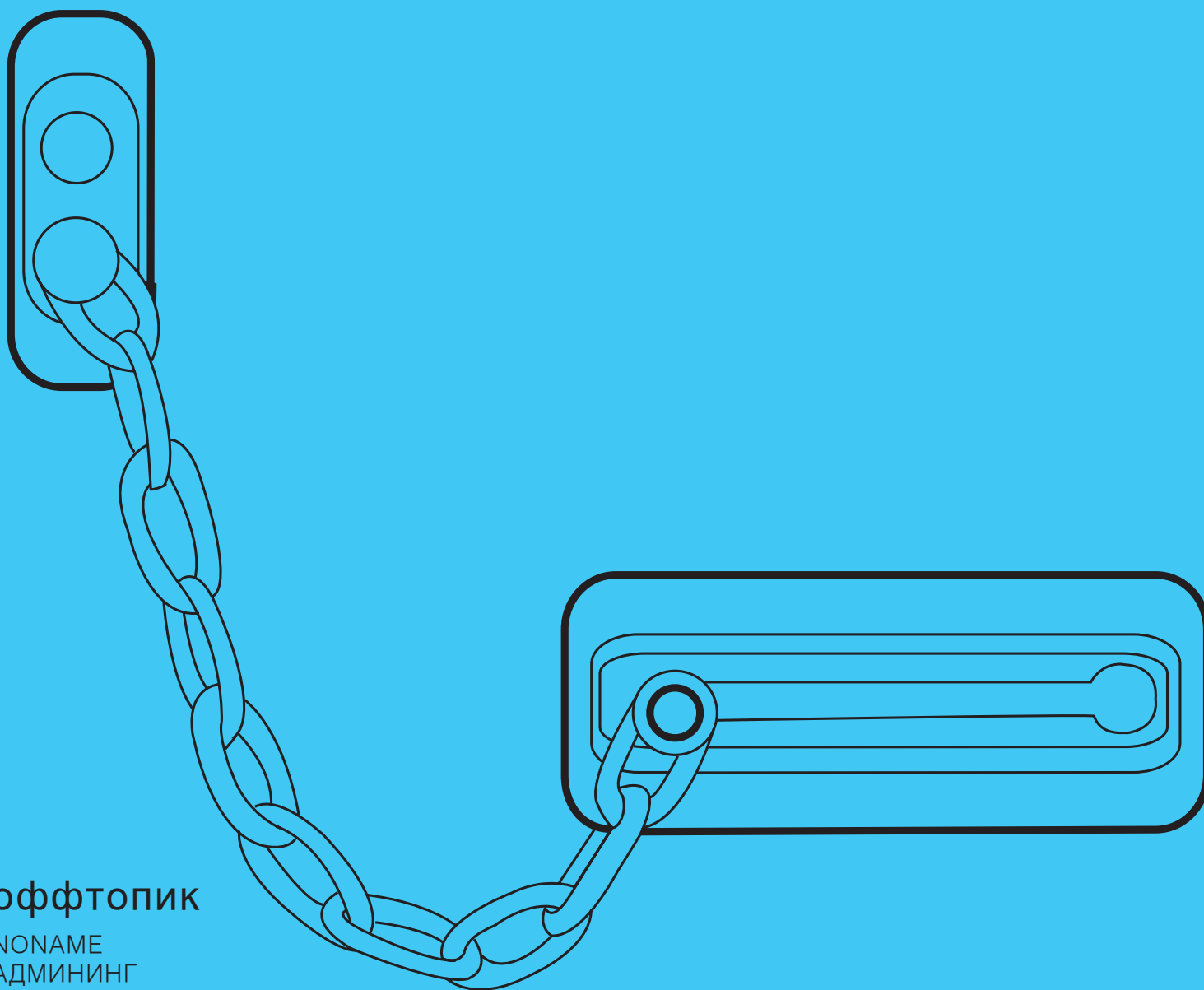
* Постоянно
обновляемый
ассортимент



Тел.: (095) 780-8825
Факс.: (095) 780-8824

www.gamepost.ru





оффтопик

NONAME
АДМИНИНГ
ВЫ ХОТЕЛИ АТИ?
PLEXTOR
Е-МЫЛО
НОЧНАЯ РАБОТА

попаме

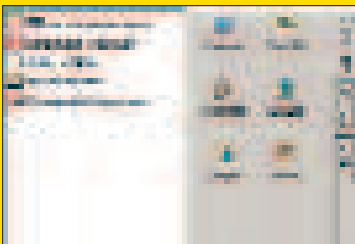
СВЕЖИЙ СОФТ ОТ NNM.RU

ID(C (DOC@NNM.RU)

MIDBUT PRO 1.10 BETA

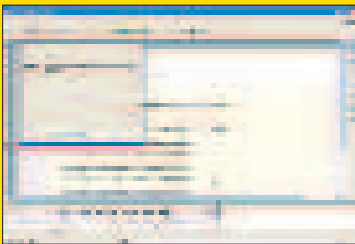
Программа цепляется на среднюю кнопку мыши (колесико) и отображает запущенные приложения (включая все скрытые), имеет свою панель быстрого запуска. Несмотря на то, что существует множество ее аналогов, MidBut кажется единственной полезной.

Кстати, написана разработчиком с www.nnm.ru, что не может не радовать. Но еще больше радует то, что она бесплатна.



SCREEN FLASH PROFESSIONAL 1.62

Программа ScreenFlash для захвата действия из любой части экрана и звука плюс для сохранения во flash-файл (*.swf). Но это еще не все. Вдобавок тебе будут доступны возможности по редактированию ролика:



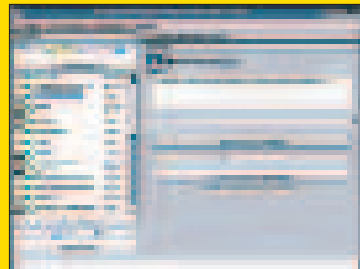
добавление кнопки, звука, изображений и текста.

Также есть возможность создавать объединенные диалоговые демонстрационные примеры. Идеально подходит, например, для создания интерактивных файлов помощи к программным продуктам.

NIKSAVER 1.4

NikSaver эффективно решает три важнейшие проблемы: сохранение настроек, их резервирование и перенос на «другой» компьютер.

Программа позволяет без проблем сохранить всю твою рабочую среду: от настроек программ, игр, операционной системы до рабочего стола, адресной книги и личной корреспонденции.



TASKSWITCHXP 2.0

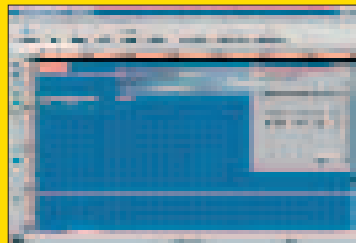
Переключатель задач — отличная альтернатива стандартному невзрачному окошку Windows, которое появляется по <Alt>+<Tab> (или <Alt>+<Shift>+<Tab>). TaskSwitchXP использует визуальные стили оформления Windows XP/2003 («Свойства экрана»> «Оформление», «Стиль Windows XP») и предоставляет воз-

можность предпросмотра выбранного окна. Возможно управление программой с помощью горячих клавиш, а также из командной строки. Интерфейс — многоязычный.



NETOBJECTS FUSION 8

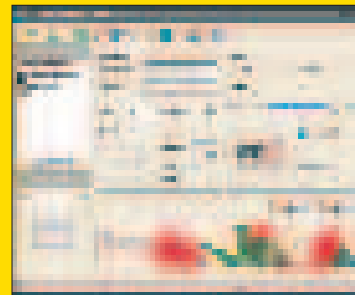
Для тех, кто хочет не вникать в подробности HTML, а просто создать собственный сайт своими руками за короткое время, NetObjects Fusion 8 — идеальный инструмент для экспериментов. С каждой новой версией в программе появляются новые профессиональные возможности не только для создания сайтов, но и для легкого управления ими.



BATCH WATERMARK CREATOR 3.2

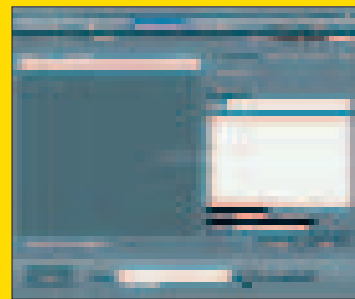
Программа, позволяющая оставлять свою подпись на изображениях. С по-

мощью таких «ватермарков» можно, например, добавить на все рисунки web-сайта надпись с его адресом. Программа умеет накладывать текст, изображение, цвет, логотипы, управлять их прозрачностью и т.д.



TAGSCANNER 4.9

Мощная программа для организации музыкальных архивов и управления ими. TagScanner переименовывает музыкальные файлы различных форматов так, чтобы в их имени содержалась информация из тегов. Или наоборот, позволяет сгенерировать тег по имени файла или директории. Плюс информация о тегах может быть получена через интернет-БД freedb.org.

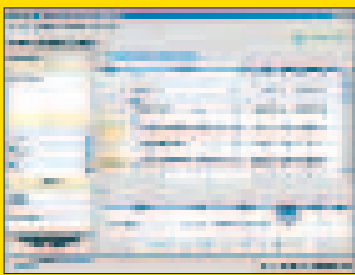


Программа от русских производителей, соответственно бесплатна (каждый раз, когда слышишь такое, охватывает гордость за бескорыстных нищих «русских производителей» — прим. SkyWriter'a).

LIMEWIRE V4.9

Вышла свежая версия программы LimeWire, предназначенной для поиска файлов любых типов и обмена ими между пользователями.

Основываясь на протоколе Gnutella, LimeWire позволяет подключаться к любым сетям обмена файлами, использующим те же самые принципы построения.



REGDOCTOR 1.42

Новая версия программы из серии «твикер системного реестра». Находит ошибки, исправляет, удаляет и т.д. Работает быстро и качественно. Имеет легкий понятный интерфейс. Если тебе захотелось сменить свой стильчик реестра, то, пожалуй, самое время сделать это. Работает под Windows 95/98/ME/2000/XP.



AVEDESK 1.3

«Выкинь свой Konfabulator» — девиз AveDesk. Программа позволяет заполнять рабочий стол динамическими виджетами. Впрочем, что тут расписывать? Сам все видишь на скриншоте...

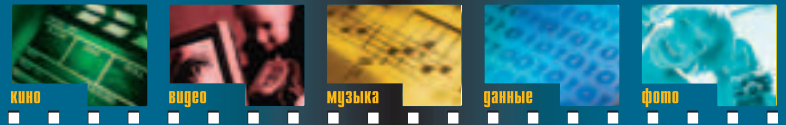
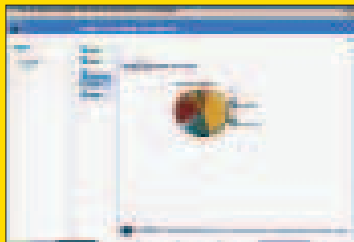


F-SECURE ANTI-VIRUS CLIENT SECURITY 6

Новая версия легендарного (оказывается) антивируса. По сравнению со старой версией, понравился быстрый доступ к настройкам через иконку монитора. Понравилось и то, как F-Secure ищет гадов — уверенно, без промахов. Есть много эвристических срабатываний, во многом благодаря одному из трех его движков — F-prot (еще есть AVP и Orion). Очень понравилось окно, большое и информативное, которое всплывает после обнаружения заразы резидентным монитором, а также то, что предлагается сделать дальше. Не обиду вниманием и то, что в антивирусе есть собственная база вирусов, троянов и червей. Что я имею в виду? Ты нашел вирус, например Melissa, сразу же нажимаешь кнопку и переходишь к описанию этого вируса.

В антивирусе есть утилита BackWeb, с помощью которой ты обновляешься. После установки F-Secure прекращается твоя забота о нем: сразу же приступает к работе, и ты практически не замечаешь его.

Обновления выпускаются ежедневно. Стоит еще заметить, что пользователями F-Secure являются: NASA, US Air Force, Yahoo, US Department of Defense Medical Branch, US Naval Warfare Center, San Diego Supercomputer Center, Lawrence-Livermore National Laboratory, IBM, Unisys, Siemens AG, EDS, Cisco, Nokia, Sonera, UUhet Technologies, Boeing, Bell Atlantic, MCI.



БУДЬ ВПЕРЕДИ — ПИШИ DVD!

ПИШУЩИЕ DVD±R/RW ПРИВОДЫ PLEXTOR НА ШАГ ВПЕРЕДИ ВСЕХ



PX-760A

- Запись двухслойных DVD-дисков
- Самые высокие скорости записи без ошибок
- Непревзойденное качество аудио-декомпрессии, воспроизведения и записи
- Большой объем буфера — 2 Мб, малое время доступа — 100 мс (CD), 150 мс (DVD)
- Комплексная технология интеллектуальной записи Intelligent Recording
- Фирменные технологии PLEXTOR для качественной записи данных и музыки, увеличения емкости дисков, защиты данных, бесшумной работы
- PlexEraser: фирменная технология уничтожения данных, применяемая в CD-R и DVD-дисках для повышения безопасности

ПИРИТ — официальный дистрибутор PLEXTOR в России:

Компьютерный салон на Профсоюзной: (095) 785-55-54;
 ПИРИТ-Дистрибуция: (095) 97-43210;
 ПИРИТ Санкт-Петербург: (812) 712-65-02

Приобрести продукцию PLEXTOR можно в следующих компаниях:

Москва: Катюша — 510-55-80, НИКС — 974-33-33, NT Computer — 970-19-30, Радиокomплект — 953-81-78, Ultra Electronics — 775-75-66, USN Computers — 775-82-02

Барнаул: НЭТА — 23-10-00; Воронеж: РЕТ — 77-93-39;
 Кемерово: НЭТА — 35-59-09; Красноярск: Ками-Красноярск — 63-28-63, НЭТА — 59-43-53; Новокузнецк: НЭТА — 35-77-33;
 Новосибирск: НЭТА — 54-10-10; Омск: НЭТА — 23-45-54

Объединенная розничная сеть POLARIS и Техмаркет Компьютерс: (095) 755-55-57

Интернет-магазины: www.dostavka.ru, www.pchome.ru



www.pirit.ru
 www.ddp.ru
 www.plextor.ru



admining

ВОССТАВШИЙ ИЗ ДИСКА

ГОТОВ ПОСПОРИТЬ, ЧТО ПОСЛЕ МОЕЙ ПЕРВОЙ СТАТЬИ ТЫ УЖЕ ОСВОИЛСЯ СО СВОИМ НОВЫМ СЕРВЕРОМ И ПОНЯЛ, ЧТО ЗА КРАСИВЫМИ ХР'ШНЫМИ «НАВОРОТАМИ» СКРЫВАЕТСЯ НЕ ТАК УЖ МАЛО. СРЕДИ НИХ, ЕСЛИ ХОРОШЕНЬКО ПОКОПАТЬСЯ, МОЖНО ВЫЛОВИТЬ ЦЕЛУЮ УЙМУ НАСТРОЕК | **АЛЕКСАНДР ПРИХОДЬКО (SANPRIN@MAIL.RU)**

день второй Итак, день второй. Ты пришел на работу, полез посмотреть, что творит твой сервер. Вроде бы стоит, работает, но толку от него не дожدهшься до тех пор, пока не населишь его тварями разумными, папками и правами. Пойдем по пути наименьшего сопротивления. Диск C:\ уже настроен, теперь займемся вторым, девственно чистым диском E:\. Для тех, кто только что включил телевизор, напомним, что диск E:\ представляет собой массив из четырех SCSI-дисков (RAID 5) и создан только для хранения файлов пользователей, программ, фильмов, музыки и т.д.

Прежде чем создавать пользователей, создадим структуру нашего хранилища. Все будет просто и логично. Достаем из широких штанин черновик, где предварительно прикинута структура предприятия, и переносим ее на диск. Условимся, что в предполагаемой конторе есть три подразделения: начальство (группа HEAD), бухгалтерия (группа «Бухгалтерия»), экономисты (группа «Экономисты»). Вот такая странная контора. Итак, создаем на диске E:\ папку USERS, внутри нее три папки по именам групп: HEAD, «Бухгалтерия» и «Экономисты».

Внутри каждой групповой папки создаем папки по фамилиям пользователей, входящих в эту группу. Сделать это просто, а объяснить понятно — сложно, но надеюсь, ты еще не потерял нить повествования, все правильно сделал и уже имеешь в корне на диске E:\ всего одну папку USERS, зато внутри нее целый куст (дерево) папок. Пользователей пока нет, но про будущую политику безопасности мы подумаем сразу. Требуется, чтобы пользователь мог творить со своей личной папкой что угодно, но только не удалять ее. Реализуем это довольно простым способом. Откроем блокнот (в смысле Notepad) и сохраним файл под именем nokill.txt, пусть пока он полегит в корне диска E:\ — еще пригодится.

Теперь я объясню идею построения корпоративной политики безопасности на уровне разрешений NTFS. Имеется групповая папка, внутри которой — папки пользователей. В корне групповой папки всем членам группы не запрещено ничего, кроме просмотра папок других пользователей. Также всем гарантируется, что до их личных папок не доберутся чужие глаза (ну ты не говори им, что остаешься ты — администратор). Пользователи группы могут видеть только свою групповую папку, в чужие группы они не попадают.

куда пойдем сегодня?

- СОЗДАДИМ ПАПКИ ДЛЯ ПОЛЬЗОВАТЕЛЕЙ, ФАЙЛ «НЕ УБИЙ»;
- ПОДНИМЕМ ДОМЕН;
- РАЗВЕРНЕМ ACTIVE DIRECTORY;
- СОЗДАДИМ ГРУППЫ;
- РАЗРУЛИМ NTFS-РАЗРЕШЕНИЯ;
- ПОНЯТИЕ ДОМЕННОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ, КВОТИРУЕМ ДИСК;
- ТЕНЕВОЕ КОПИРОВАНИЕ — ЗАЧЕМ ОНО И С ЧЕМ ЕГО ЕДЯТ.

Однако нашей организации необходима папка, в которую может залезть любой желающий. Предоставим же ей такое счастье.

Создаем в корне диска E:\ папку с громким именем «Обмен». Далее предоставим всем пользователям полные права на нее (надеюсь, ты не забыл, что пользователей пока нет и их права распределяем только в уме). Потратить еще некоторое количество времени и каждому пользователю в его личную папку поместить файл nokill.txt, выставить ему атрибут «Скрытый», права на него пока не трогать. В принципе, пока разрешениями NTFS мы не занимались совсем. Время, затраченное на создание файловой структуры, с лихвой окупится после поднятия домена.

поднимаем неподъемное Наступило время заняться серьезным делом — поднимать домен. Ты знаешь, почему у Буратино дерево не выросло? Потому что бестолковая лиса Алиса сказала ему не ту команду: вместо «Preks-Feks-Пекс» нужно было набирать в командной строке «DCPROMO», и тогда даже не дерево — целый лес бы вырос.

Поехали. Start> Run, в строке Open набрать «dcpromo» — попадаем на Active Directory Installation Wizard. Нажать Next, внимательно прочитать предупреждение о том, что старые оси Windows 95 и Windows NT4 не смогут подключиться к домену, который работает под управлением Win2k3 Server. На следующей страничке выбираем Domain controller for a new Domain, затем Next (соглашаемся на создание нового леса). Затем предлагается сконфигурировать DNS (ну не работает AD без DNS) — согласиться. Далее предупредят о необходимости откорректировать сетевые параметры, в ответ залезть в свойства протокола TCP/IP, в поле Preferred DNS Server укажи IP-адрес своего же сервера. Теперь необходимо придумать имя этому новому домену.

А сейчас лирическое отступление. Возможности операционной системы

Windows 2003 Server, вопреки распространенному мнению, очень широкие. Когда в офисе разворачивается AD, предполагается, что в данной конторе работает около 10 000 человек, поэтому механизмы настройки и аудита такие серьезные. При создании пользователей в контексте AD каждый пользователь получает свой e-mail-адрес — `pirkin@твойдомен.провайдер`. Если ты поднимаешь домен и у тебя есть реальное доменное имя, то в название домена должно быть введено именно оно. Но мы рассматриваем ситуацию, когда домен поднимается в локальной небольшой сети, так что назначаем любое имя. Я, например, обхожусь двухбуквенным именем. Соответственно, и DNS-зона, которую поднимем, будет кукольной.

Итак, имя нашли. В ответ пришло гнусное предупреждение о том, что имя должно походить на `domain.microsoft.com` — проигнорировать, нажать Yes. После минуты обиженного молчания Windows соглашается с нашим именем и даже угодливо предлагают свой вариант Domain NetBIOS Name — соглашайся. Далее следует создание каталогов для размещения базы данных AD. Существует мнение, что базу NTDS лучше не держать на системном диске, чтобы не снижать быстродействие. Когда в AD сидит 10 000 пользователей, это заметно, но в нашей провинциальной сети на 10-100 пользователей особого простора в скорости мы не заметим, так что оставляй все по умолчанию. Держать на системном диске каталог SYSVOL тоже не рекомендуется. Далее получаем сообщение об ошибке настройки зоны DNS — выбрать пункт «I will correct the problem later by configuring DNS manually» (Advanced).

Теперь нарываемся на очередную швабру — Permission. Нужно честно ответить на вопрос о том, есть ли в сети машины под управлением старых операционнок или только под Windows 2000 и выше. В нашей организации все круто, у всех пользователей стоит XP или Win2K, поэтому выбираем следующий вариант: Permission compatible only with Windows 2000... Далее вводим пароль для режима восстановления (этот режим — отдельная тема политики безопасности). В следующем окне читаешь о том, что уже натворил, давишь Next и идешь спать, ибо начинается шаманский танец «Конфигурирование Active Directory». После просмотра танца — кнопка Finish> Restart now...

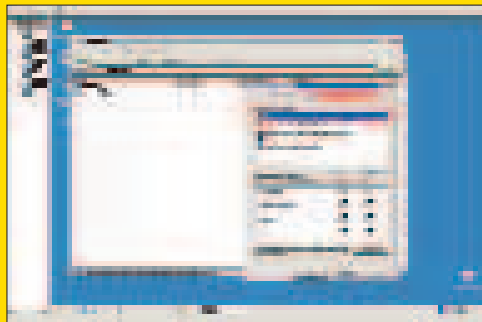
ребут После перезагрузки в окне Logon появилась дополнительная строчка Logon to, где уже прописано имя твоего домена. В закладке Administrative Tools появилась целая куча новых инструментов. «Да будет Свет!» уже было сказано — теперь начнем заселять наш новый лес.

Start> Programs> Administrative Tools> Active Directory> Users and Computers> Users. Ба-а, сколько тут новых пользователей появилось! С ними разберемся позже, пока начнем создавать группы (папки для них уже сделаны). Правая кнопка мыши на Users, меню New Group, написать «HEAD» и выбрать область действия группы (Group scope) Global.

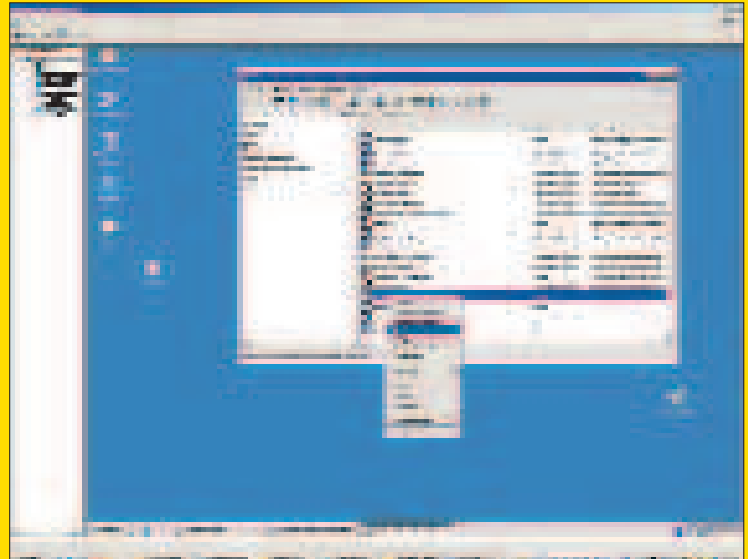
Небольшое техническое отступление. Есть очень хорошая книга Ф.Зубанова «Active Directory», в которой очень толково написано, для чего служат определенные области действия групп. Я оставлю тонкости, можешь прочитать сам, если книгу найдешь. Конец отступления.

Таким же методом заводим группы «Бухгалтерия»

и «Экономисты». Главное правило при назначении любых прав гласит: «Все права назначаются через групповые политики». Кратко поясню, что доступ ко всем объектам осуществляется через SID (идентификатор безопасности), и если на какой-нибудь файл ты будешь назначать пра-



Потерянный
пользователь



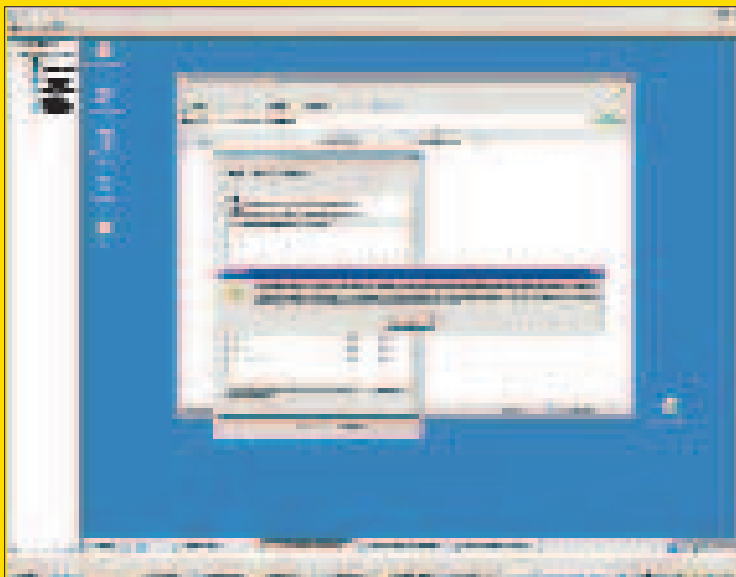
Сброс пароля

ва конкретному пользователю, а затем удалишь пользователя из системы, то на этом файле останется висеть SID пользователя. Для того чтобы кого не происходило, доступ ко всем ресурсам осуществляется через группы, так как в этом случае операционная система ставит на объект SID группы и, соответственно, в базе AD не появляется лишней записей. Пример потерянного пользователя смотри на рисунке.

населяем эдем живностью Заводим пользователей. Все так же, как и при создании групп, только выбираем User. Лучше не полениться и полностью заполнить все поля карточки пользователя. Представь, что однажды лень таки пересилила тебя, примерно через полгода смотришь на учетную запись «Света» и мучительно вспоминаешь, к какой из 12-ти работающих в конторе Свет относится эта запись. Мораль: лень в себе нужно контролировать жестко. Итак, тупо заполняем карточки пользователей по списку, выданному кадровой службой. Можно пока не напрягаться с паролями и правами и заниматься только бюрократией. Завели. Переходим к правам и обязанностям.

Я опишу настройку прав на примере одной группы и одного пользователя, для остальных будет аналогично. Берем пользователя Иванова из группы HEAD. Открываем оснастку Active Directory Users and Computers. Двойной щелчок на пользователе «Иванов», попали в свойства, выбрать закладку Member of. Там светится одна группа Domain Users, нажать кнопарик Add> Advanced> Find Now, в открывшемся списке выбрать группу HEAD. Если время жизни паролей для тебя не критично (ты не занимаешься жуткой коммерческой тайной и т.д.), то, перейдя на закладку Account, отметь галочкой Password never expires. Если не хочешь, чтобы пользователь сам изменял пароль, рядом ставишь галочку напротив User cannot change password. Возможности по настройке прав пользователя в системах Windows Server очень большие. Если внимательно изучить свойства пользователя, то можно найти массу способов ограничить его права в домене. А если изменить пароль конкретному пользователю, щелкай правой кнопкой мыши на пользователе и в выпавшем меню выбирай Reset Password.

Заниматься этим придется очень часто, если ты позволишь пользователям самим менять пароли :). Как говорят французы, се ля ви. Либо пользователи сами изменяют пароли и забывают их, зато кроме пользователя и тебя на его машину никто не влезет, а ты с завидной периодичностью будешь сбрасывать пароли подопечным, либо ты сам прописываешь пароли и дальше проблема пользователя, что делать с ним — приклеить к монитору на стикере или запомнить.



Удалить
пользователя
нельзя

психологическое отступление Чем сложнее и строже политика безопасности, тем чаще в твою безопасность вмешивается человеческий фактор. Не хочется переходить на личности, но в одном московском банке установили аутентификацию на вход в систему по ключам Touch Memory. Через два месяца ребята, которые устанавливали это все, пришли в банк по мелким делам и чуть не заработали инфаркт: почти на всех системных блоках висели приклеенные на скотче ключи Touch Memory. На гневное замечание о нарушении безопасности работники банка ответили: «Зато так мы не теряем эти ключи». Любая безопасность бессильна перед человеческим фактором. Если пароль очень длинный, пользователь напишет его на бумажке и оставит возле монитора. Я не призываю, конечно, наплевать на безопасность, но попробуем свести вред человеческого фактора к минимуму. Попробуем построить домен так, чтобы не бояться потерять любой компьютер домена плюс чтобы сам домен никак не пострадал.

эта долька для ежа... Теперь размещаем наших пользователей по группам «Ляпкин, Тяпкин, Пупкин» — «Экономисты», «Иванов, Петров, Сидоров» — HEAD, «Балаганов, Бендер, Козлевич» — «Бухгалтерия».

Займемся NTFS-разрешениями. Для этого заходим на диск E:\ в папку HEAD>Users, далее папка «Иванов».

На файле nokill.txt правой кнопкой мыши, Properties> Security, в поле Group or user names удалить всех, кроме Administrators (это делается через кнопку Remove). И тут мы получаем сообщение о невозможности удалить пользователя, потому что разрешения NTFS на этот объект наследуются от родительского, то есть от диска E:\.

Напротив надписи «For special permissions...» нажимаем кнопку Advanced. В открывшихся свойствах на первой закладке наблюдаем все действующие разрешения. Убираем галочку напротив надписи «Allow inheritable permissions...», так как Windows по умолчанию распространяет все разрешения с родительского объекта на дочерний. Если ты создаешь каталог и назначаешь на нем какие-нибудь права, а позже внутри этого каталога создается файл или другой каталог, то вновь созданные файлы/папки получают те же права, что и родительские. Так вот чтобы спокойно рулить правами на дочернем, просто снимаем ту галочку. В результате Windows выдает запрос: «Что сделать с уже имеющимися правами?» Их можно скопировать либо удалить — выбираем «Скопировать».

Теперь, вернувшись на предыдущую страничку, спокойно удаляем всех пользователей, кроме группы Administrators. Теперь файл nokill.txt можешь уда-

лить только ты — Administrator. При этом сам пользователь «Иванов» не сможет убить свою папку, так как она не пуста.

Я рассказываю так подробно, чтобы потом не возвращаться к этому вопросу. А сейчас работаем аналогично с папкой «Иванов»: правой кнопкой

Properties> закладка Security> Advanced, снова снять галочку, скопировать разрешения, возвратиться, удалить всех, кроме группы Administrators. Добавить пользователя «Иванов», дать ему разрешение Full Control. Теперь в папку может попасть только «Иванов» и Administrators. Все то же самое проделать со всеми пользователями и их папками. А никто и не говорил, что будет легко...

Теперь разберемся с папкой «Обмен». Так же в нее помещаем nokill.txt, отмечаем Share This Folder> Permissions и даем полное разрешение на папку учетной записи Everyone. Далее идем на соседнюю закладку Security и чуть

изменяем права пользователю Users: отмечаем Full Control. Теперь все пользователи, зарегистрированные в домене, могут заходить в папку «Обмен», создавать и удалять там любое содержимое, кроме файла nokill.txt и, соответственно, самой папки «Обмен».

Все, что описывается в этой статье, работает, но полное понимание всех механизмов действующих разрешений немного сложнее. Например, на папке «Обмен» мы имеем два вида разрешений: одно разрешение — Sharing, вторая группа разрешений — Security. Так вот, результирующее разрешение будет пересечением двух этих разрешений. На папке «Обмен» и по первому, и по второму виду разрешений имеем «Полный доступ», поэтому все пользователи могут делать что захотят. Если бы по одному разрешению мы имели «Полный доступ», а по второму, например, «Только чтение», то результирующим было бы разрешение «Только чтение» (применяются максимально ограничивающие разрешения).

вам сколько байтов отгружать? Теперь рассмотрим понятие «квоты».

Первое, что приходит на ум, если слышишь это слово, — размер чего-то. Все верно, «квота» относится как раз к размерам и пределам. Для того чтобы твой сервер не стал свалкой ненужных файлов, предусмотрена возможность назначить каждому пользователю максимальную квоту, которую он может занять на дисковом пространстве сервера. По умолчанию кватирование диска отключено, и поэтому каждый пользователь может занять своими данными все пространство — нам такое не подходит. Среднестатистическим клеркам для хранения их средних Word'овских и Excel'овских файлов хватит и ста мегабайт дискового пространства. Но ты сам примешь решение, сколько отрезать от общего пирога определенным людям, исходя из потребностей пользователей и размера пирога. Включаем квоту: правая кнопка мыши на диске E:\> Properties> Quota, отмечаем Enable quota management> Deny disk space to users exceeding quota limit.

Дальше все понятно и без слов: отмечаем Limit disk space to, устанавливаем

саму квоту (пусть будет 100 Мб). Чтобы вовремя предупреждать пользователя о том, что заканчивается место, отведенное для его нужд на диске, вводим параметр в поле Set warning level to (ставим 98 Мб). Теперь пользователь получит предупреждение при прохождении контрольной точки в 98 Мб. Далее если любишь почитать логи, то отмечай чекбоксы, когда пользователь превысит квоту и пройдет контрольную точку. Но я думаю, что для тебя это лишнее чтение: на контроллере домена всегда и так есть что почитать в логах. Далее жмешь кнопку Quota Entries и в открывшемся окне давишь

на белый листик в левом углу.

Установка квоты на
пользователя



так сказал Заратустра

Я ВДРУГ РЕШИЛ ПОФИЛОСОФСТВОВАТЬ НА ТЕМУ ИЗОБРЕТЕНИЯ ПАРОЛЕЙ. СУЩЕСТВУЕТ КУЧА СПОСОБОВ ВЗЛОМАТЬ ЧЕЙ-НИБУДЬ ПАРОЛЬ: СОФТ, СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ И МНОГОЕ-МНОГОЕ ДРУГОЕ. ВСЕГДА СМЕЮСЬ, КОГДА УЗНАЮ, ЧТО МОИМ ПОДОПЕЧНЫМ СНОВА ПРИШЛО ПИСЬМО ЯКОБЫ ОТ МЕНЯ (АДМИНИСТРАТОРА ПОЧТОВОЙ СИСТЕМЫ): «Я, АДМИНИСТРАТОР ПОЧТОВОЙ СИСТЕМЫ, УТЕРЯЛ БАЗУ ДАННЫХ ПАРОЛЕЙ И ПРОШУ ВЫСЛАТЬ МНЕ PASSWORD ОТ ВАШЕГО ПОЧТОВОГО ЯЩИКА». ОСОБЕННО СМЕШНО ТО, ЧТО НЕКОТОРЫЕ МОИ ПОЛЬЗОВАТЕЛИ ИМЕЮТ ПРОБЛЕМЫ И С РУССКИМ ЯЗЫКОМ, А ПИСЬМА-ТО НА АНГЛИЙСКОМ ПРИХОДЯТ :). ВЕСЕЛО, В ОБЩЕМ. ВПРОЧЕМ, РУССКИЕ (И ВСЕ БЫВШИЙ СССР) ОТЛИЧАЮТСЯ СВОЕЙ СООБРАЗИТЕЛЬНОСТЬЮ ОТ АМЕРИКАНЦЕВ (И ОСТАЛЬНЫХ БУРЖУЕВ), ПОЭТОМУ И ПАРОЛИ У НАС ДРУГИЕ. ВСЕ СПЕЦЫ В ОДИН ГОЛОС СОВЕТУЮТ ИСПОЛЬЗОВАТЬ ТАК НАЗЫВАЕМЫЕ КОМПЛЕКСНЫЕ ПАРОЛИ — ВПЕРЕМЕШКУ БУКВЫ-ЦИФРЫ И СИМВОЛЫ. НАПРИМЕР, ВМЕСТО БУКВЫ «А» ИСПОЛЬЗУЕТСЯ СИМВОЛ «@», А ВМЕСТО БУКВЫ «О» — ЦИФРА «0» И Т.Д. ПО-МОЕМУ, ЗАПОМИНАТЬ ТАКОЕ ПРОБЛЕМАТИЧНО. Я ПОЛЬЗУЮСЬ ДРУГИМ СПОСОБОМ. КАК ВАРИАНТ, ВЫБИРАЕШЬ ДЛИННОЕ СЛОВО И, ГЛЯДЯ НА РУССКИЕ БУКВЫ, НАБИРАЕШЬ В АНГЛИЙСКОЙ РАСКЛАДКЕ (ЕСЛИ СЛОВО РУССКОЕ) И НАОБОРОТ. ВПЕРЕМЕШКУ ДОЛЖНЫ ИДТИ ПРОПИСНЫЕ И СТРОЧНЫЕ БУКВЫ. ЕСЛИ НУЖНО ИЛИ ХОЧЕТСЯ ИЗМЕНЯТЬ ПАРОЛИ ЧАСТО, ВОСПОЛЬЗУЙСЯ СТАРЫМ ДЕДОВСКИМ СПОСОБОМ: БЕРЕШЬ ЛЮБУЮ ХОРОШО ЗНАКОМУЮ ПЕСНЮ И В ПЕРВЫЙ ДЕНЬ НАБИРАЕШЬ КАК ПАРОЛЬ ПЕРВУЮ СТРОКУ КУПЛЕТА, НА СЛЕДУЮЩИЙ ДЕНЬ — ВТОРУЮ СТРОЧКУ И ТАК ДО ОКОНЧАНИЯ ПЕСНИ. ЗАТЕМ ПЕРЕХОДИШЬ К СЛЕДУЮЩЕЙ ПЕСНЕ. А ЕСЛИ СТРОКИ КУПЛЕТА ПЕРЕМЕЖАТЬ СО СПЕЦСИМВОЛАМИ, ТО КТО-ТО ВСТУПИТ В ЛЮБОВНУЮ СВЯЗЬ САМ С СОБОЙ, ПЫТАЯСЬ ПОДОБРАТЬ ТВОЙ ПАРОЛЬ. ТАК ЧТО И В НАШЕМ ДЕЛЕ ЕСТЬ МЕСТО ДЛЯ ЛЮБВИ :). ЕДИНСТВЕННОЕ, К ЧЕМУ НЕ ПРИЗЫВАЮ, — ЭТО ИСПОЛЬЗОВАТЬ ТОЛЬКО ТЕ СПОСОБЫ, КОТОРЫЕ ОПИСАЛ Я. ЕСЛИ ПРИЕМ СОЗДАНИЯ ПАРОЛЯ, ДАЖЕ САМЫЙ ЗАКРУЧЕННЫЙ, СТАНОВИТСЯ ПРАВИЛОМ, ОН ТУТ ЖЕ ТЕРЯЕТ СВОЮ АКТУАЛЬНОСТЬ: ДОСТАТОЧНО УЗНАТЬ КРУГ МУЗЫКАЛЬНЫХ ИНТЕРЕСОВ ПОЛЬЗОВАТЕЛЕЙ, И УЖЕ ВРЕМЯ ПОДБОРА ПАРОЛЕЙ НАМНОГО СОКРАЩЕНО... ПОНЯЛ НАМЕК :-)?

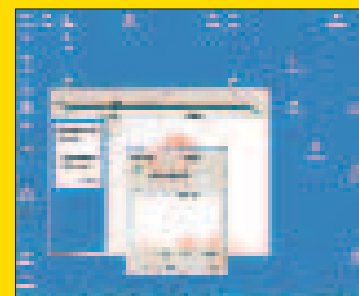
Дальнейшую процедуру ты и сам знаешь не хуже, чем таблицу умножения. Выбираешь пользователя, выставляешь ему ограничения. Существует всего одна проблема при квотировании дисков. Правда, это проблема твоих пользователей, но... По твоим настройкам пользователь может бросать

свои файлы в три папки: в корень групповой папки (HEAD), в свою личную папку («Иванов») и в «Обмен». Так что если он набросает файлов на 100 Мб в папку «Обмен», то очень удивится, когда не сможет положить нужный документ в личную папку. Дабы он не мучил тебя своими подозрениями, среди личного состава вверенного тебе боевого подразделения проведи разъяснительную беседу на тему «Своевременная уборка вверенных территорий как залог наличия свободного места и чистой совести». Пользователи, которые не пользуются ничем, кроме Word'a и Excel'a, вряд ли доставят тебе много хлопот, но любителей МРЗ'шек ждет глубокое разочарование. Никто не мешает тебе увеличивать квоту для любимых подопечных. Умные книги советуют раздавать квоты не пользователям, а группам. Прислушайся к совету, и рулить будет проще.

первый после бога И напоследок: не забудь включить теневое копирование диска, если хочешь, чтобы пользователи молились на тебя как на шамана. Разъясню суть теневого копирования. При его включении и при настройках по умолчанию состояние всего диска сбрасывается в теньевую копию два раза в сутки (рекомендую настроить утром и вечером), постоянно будет храниться откат предыдущего дня в его двух состояниях: на конец рабочего времени и на начало нового дня конторы. Если пользователь снес на сетевом диске годовой отчет и уже начал прилаживать к потолку намыленную веревку, ты подходишь к нему и, придерживая стул под ним, чтобы он (стул) не упал раньше времени, восстанавливаешь удаленный файл. Теневое копирование позволяет «откатиться» назад на какое-то время. Глубина отката задается при тенево копировании указанием размера, отведенного под тенево копирование. Естественно, чем больше места, тем больше откатов возможно. Восстановление происходит через «Проводник»: правая кнопка мыши на сетевой папке, в контекстном меню выбрать Previous Versions.

Далее в открывшемся окне выбираешь действие: View, Copy или Restore. Для корректности отката спроси у пользователя, что именно он потерял, и мастерским кликом мыши свергни его в эйфорию. На сегодня все. В следующий раз поговорим об именах и адресах, для настройки поднимем DNS и WINS и чуть-чуть пощупаем протоколы

Восстановление удаленных файлов на сетевом ресурсе



Отдых, который вам нужен

ИГИДА АЭРО
Т. 945 3003
945 4579

Лиц. ТД № 0025315

АВЦ
Т. 508 7962
504 6508

ВЫ ХОТЕЛИ АТІ?

список тестируемого оборудования:

Sapphire Radeon X700 Pro Toxic | Sapphire ATI Radeon X1300
Sapphire ATI Radeon X800GTO2 | Gigabyte Radeon X800 (RX80256D)
PowerColor X800GT | PowerColor X800GT EVO | MSI RX1300PRO-TD256E
HIS ATI Radeon X800GTO | GeCube Radeon X800GTO

ПРЕПАРИРУЕМ MIDDLE-END RADEON'Ы

СКОЛЬКО УЖЕ ТЫ ВИДЕЛ ЭТИХ САМЫХ ТЕСТОВ, ПОСВЯЩЕННЫХ ВИДЕОКОНТРОЛЛЕРАМ ДАЖЕ НА СТРАНИЦАХ НАШЕГО ЖУРНАЛА. ОДНАКО ИМЕННО ЭТОТ ОБЗОР МЫ РЕШИЛИ ПОСВЯТИТЬ ФАНАТАМ АДАПТЕРОВ НА ЧИПАХ ОТ АТІ. ВОЗМОЖНО, ТЫ УЖЕ ОПРЕДЕЛИЛСЯ, ЧТО ТЕБЕ НУЖЕН ИМЕННО RADEON, ОДНАКО КАКОЙ ИМЕННО, ТЫ ЕЩЕ НЕ ЗНАЕШЬ. МЫ ПОПЫТАЛИСЬ ПОМОЧЬ ТЕБЕ РАЗОБРАТЬСЯ С ПОРЯДКОВЫМ НОМЕРОМ ТВОЕГО ВИДЕОКОНТРОЛЛЕРА — ТОГО САМОГО АДАПТЕРА, КОТОРЫЙ НЕ ТОЛЬКО БУДЕТ ПО КАРМАНУ, НО ЕЩЕ И ПОРАДУЕТ ПРОИЗВОДИТЕЛЬНОСТЬЮ, СРАВНИМОЙ С ПОКАЗАТЕЛЯМИ МЭТРОВ РЫНКА ГРАФИЧЕСКИХ КАРТ. ОДНАКО ПРЕДУПРЕЖДАЕМ, ЧТО В ТЕСТЕ ТЫ НЕ НАЙДЕШЬ ОЧЕНЬ ДЕШЕВЫХ РЕШЕНИЙ, ТАК КАК, НА НАШ ВЗГЛЯД, НЕ ИМЕЕТ СМЫСЛА РАССМАТРИВАТЬ ИХ В УСЛОВИЯХ СОВРЕМЕННОГО РЫНКА. ОДНО ДЕЛО — ПЛАТЫ ДЛЯ ОФИСА, ДРУГОЕ — ДЛЯ ЖЕСТКОГО ИСПОЛЬЗОВАНИЯ И ОВЕРКЛОКЕРСТВА | **ЕВГЕНИЙ ПОПОВ, TEST_LAB (TEST_LAB@GAMELAND.RU)**

ТЕХНОЛОГИИ Перед рассмотрением результатов тестирования скажем пару слов о положении на рынке графических плат. В последние полгода компания АТІ постоянно находилась в позиции нагоняющего. Сначала удар был нанесен выпуском GeForce 6600GT от Nvidia. Попытка выпустить видеокарты на чипах X700 и X700 PRO провалилась, тем более что их цена была высокой. После выпуска плат на основе X800 положение АТІ несколько улучшилось, однако здесь вновь дело в цене. Все решения, способные конкурировать с Nvidia, стоят дороже минимум на \$50. Для выпуска конкурентоспособного устройства при надлежащем ценовом пороге был налажен выпуск плат на основе свежеразработанного чипа R480. По сравнению с пре-

дыдущими версиями, был повышен порог тактовой частоты, а также число работающих пиксельных конвейеров. Такие чипы получили название X850XT. Само собой, они стали заменой для плат на основе R423, то есть X800XT.

Однако они тоже не остались без дела, так как в августе этого года АТІ представила на суд публики Radeon X800GT — совершенно новый продукт для PCI-E-интерфейса. Разрешение на выпуск таких плат было доверено, по данным официального сайта АТІ, таким компаниям, как PowerColor(TUL), Sapphire, HIS и GeCube. Однако, вопреки слухам, как основа для разработки данных плат использовались не только чипы R423, но и R480. Дело в том, что тактовая частота, о которой говорилось выше, для таких устройств была по-



лучшая
покупка
лучшая покупка
по мнению редакции
СПЕЦ

ТЕСТОВЫЙ СТЕНД:

ПРОЦЕССОР: AMD ATHLON64 3200+ (SOCKET 939)
МАТЕРИНСКАЯ ПЛАТА: GIGABYTE K8-SLI
ПАМЯТЬ: PIONEER 1X1024 MB

КУЛЕР: COOLER MASTER HYPER6+
ЖЕСТАК: SEAGATE BARRACUDA IDE 80MB
ОПЕРАЦИОННАЯ СИСТЕМА: WINDOWS XP PROFESSIONAL SP2
БЛОК ПИТАНИЯ: DEFENDER ATX-450W

вышена до 475 МГц, что маловероятно для других чипов. Количество пиксельных конвейеров достигло 16-ти, из них работают только восемь, хотя для некоторых устройств, например Sapphire ATI Radeon X800GTO2, производитель гарантированно разблокировал 12 пиксельных конвейеров, то есть карта по производительности сравнима с устройствами типа X850.

Компанией Sapphire выпущен вариант платы GTO под маркетинговым названием FireBlade. В этом случае уже в заводских условиях были увеличены частоты с 400 МГц до 550 МГц для процессора, и с 900 МГц до 1080 МГц. По сравнению с устройствами типа GeForce 6600GT, графические контроллеры на основе X800GT имеют разрядность шины в два раза больше, то есть 256 бит против 128-ми, что, конечно, весьма неплохо. Также были выпущены разновидности для различных ценовых категорий с объемом памяти стандарта и GDDR3, и DDR1. Между тем, в обзоре были использованы несколько решений на основе чипов RX1300, для того чтобы ты четко различал контроллеры различных поколений.

методика тестирования Итак, шутки в сторону. Для начала определим основные требования к подопытным видеоплатам: производительность, низкий уровень шума, приятный дизайн, хорошая комплектация и, ко-

нечно же, ценовой фактор. Именно на эти критерии мы и будем опираться при проведении тестирования. Для оценки того или иного агрегата мы в первую очередь прогоняем систему на популярных бенчмарках: 3D Mark 2005 ver.1.0 и 3D Mark 2003 ver.3.4.0. Все это для двух вариантов: при включенном антиалайзинге и аннизотропной фильтрации и без них. В качестве игровых платформ были выбраны: Doom3, HL2, FarCry а также F.E.A.R — недавно появившаяся игровая платформа, которая произвела фурор среди геймеров. И конечно, все это дело прогонялось в двух режимах: при включенных антиалайзинге категории 16x, а также аннизотропии уровня 4x и, соответственно, при их отсутствии. Для некоторых карт требовалось дополнительное питание, для этого мы взяли мощный блок питания на 450 Вт. Кстати, для того чтобы производительность видеолат зависела в меньшей степени от процессора, он был разогнан до 3800+.

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ ОБОРУДОВАНИЕ РОССИЙСКИМ ПРЕДСТАВИТЕЛЬСТВАМ КОМПАНИЙ SAPPHIRE, HIS, ATI, MSI И GIGABYTE

SAPPHIRE RADEON X700 PRO TOXIC

ядро: ATI RV480
чипсет: Radeon X700PRO
шина памяти, бит: 128
объем памяти, Мб: 128
частота ядра: 425
частота памяти: 432(864)
тип памяти: GDDR-3

Заявляем сразу — это отличный выбор для ценителей соотношения цена/качество. Внешность данного графического адаптера, выполненного на чипсете Radeon X700PRO при поддержке 256 Мб DDR3 памяти, сразу бросается в глаза благодаря своему оригинальному решению: охлаждающий радиатор заключен в яркий пластиковый кожух. Во время работы вентилятора нагретый воздух сдувается в выхлопное отверстие на конце корпуса. Оригинально, не правда ли? Удивительно, но вся система работает довольно тихо и, что важно, производительно. Очень понравилось наличие в комплекте небольшой флуоресцентной лампы для украшения корпуса. Да и в самой карте имеется ультрафиолетовая подсветка. Комплект стандартный для Sapphire: пять дисков (дрова, две игры и PowerDVD 5), четыре необходимых переходника плюс мануал, не считая подсветки и крепежей. В плане компактности плата откровенно в минусе. Ты вряд ли сможешь использовать соседний PCI-порт и про блок питания не забудь — 300 Вт или более.



HIS ATI RADEON X800 GTO

ядро: ATI RV410
чипсет: Radeon X800GTO
шина памяти, бит: 256
объем памяти, Мб: 256
частота ядра: 500 МГц
частота памяти: 625 (1200) МГц
тип памяти: GDDR-3

Довольно мало компаний, таких как HIS (Hightech Information Systems), способных одновременно с погоней за деньгами делать качественный продукт. Эта команда, известная своими инновационными системами охлаждения, порадовала нас новым продуктом. Плата с интерфейсом PCI-E и памятью на 256 Мб, размещенной в восьми микросхемах Samsung (1,6 нс). Дизайн комплекса охлаждения от Arctic Cooling, IceQ II выполнен по последнему слову техники: он выполнен в форме выхлопной системы, которая обеспечивает шумовой порог в 20 дБ, что очень неплохо, а за температурой следит поставляемый с ПО драйвер. На



карте имеется дополнительный процессор, отвечающий за функцию VIVO — RAGE Theater. Питание обеспечивается не от внешнего источника — неоспоримый плюс данной платы. Если говорить о внешних портах, то тут все стандартно: DVI, D-Sub и TV-Out. В комплекте имеются все необходимые переходники и три диска. Из минусов отмечаем, как всегда, громоздкость устройства. В общем, с одним портом PCI можешь попрощаться.

POWERCOLOR X800GT EVO

ядро: ATI RV480
чипсет: Radeon X800GT
шина памяти, бит: 256
объем памяти, Мб: 256
частота ядра: 475 МГц
частота памяти: 2x490 МГц
тип памяти: GDDR-3

Компания TUL (она же PowerColor) несколько месяцев назад объявила о запуске графических контроллеров нового поколения. И вот один из них перед нами. PowerColor X800GT EVO построен на базе графического процессора R480 с пиксельными конвейерами в количестве восьми штук, с 256-разрядной GDDR3-памятью. Время выборки для данной платы составляет 1,6 нс (1050 МГц).

Рассмотрим вариант этого потрясающего агрегата с водяной системой охлаждения и с соответствующей оверклокерской памятью. Охлаждение от Thermaltake представлено отдельной платой, которая крепится на соседний PCI-слот. Тяжеленная, надо сказать, штука, да и кулер на ней при высоких скоростях шумит порядочно. Производитель гарантирует безопасный разгон до 560 МГц для ядра. Результаты по производительности тоже радуют. Тираж, в котором будет выпущен данный агрегат, сильно ограничен, скорее всего, из-за сложности производства и довольно высокой цены.



POWERCOLOR X800GT

ядро: ATI RV480
чипсет: Radeon X800GT
шина памяти, бит: 256
объем памяти, Мб: 256
частота ядра: 475 МГц
частота памяти: 2x490 МГц
тип памяти: GDDR-3

Перед нами облегченный вариант продукта PowerColor X800GT EVO, а точнее, без водяного охлаждения. Как это отражается на производительности, видно по результатам тестов. В остальном ничего не изменилось. Если говорить о внешнем виде продукта, то тут перед нами явный референс от ATI. В качестве охлаждения в данном варианте использован алюминиевый радиатор с вентилятором. При своих больших размерах такой охлаждающий комплекс работает только для основного чипа — с памятью, как ни странно, контакта нет. Сам вентилятор работает практически бесшумно, а в одном из



дисков комплекта прилагается софт для регулировки скорости вращения. Дополнительного питания не требуется. Среди внешних выходов на карте имеется два DVI и один TV-out. Плата имеет хороший разгонный потенциал, что не может не порадовать оверклокеров. Хотелось бы получить от PowerColor в будущем разблокирования пиксельных конвейеров для лучшей работы с платой и усовершенствования системы охлаждения.

MSI RX1300PRO-TD256E

ядро: ATI RV515

чипсет: Radeon X1300

шина памяти, бит: 256

объем памяти, Мб: 256

частота ядра: 600 МГц

частота памяти: 800 МГц

тип памяти: DDR2

Данный агрегат мы включили в обзор не просто так, а так как эта плата изготовлена по технологии 90 нм.

По сравнению с другими устройствами, произведенными по технологическим критериям 110, а также 130 нм, это устройство гораздо лучше справляется с трехмерными приложениями при меньших затратах, что видно очень хорошо по результатам тестирования. MSI RX1300PRO-TD256E рассчитана на порт PCI Express 16x, работает на памяти DDR2, что не очень хорошо для устройства такого уровня. Присутствует и поддержка шейдеров версии 3.0, а технология AVIVO обеспечивает максимальную четкость при формировании изображения. Такой графический контроллер позволяет пользователю работать в режиме Crossfire (аналог системы SLI), то есть при желании возможно удвоить производительность всей системы с посильными финансовыми затратами. Из минусов сразу отметим плохую систему охлаждения: маленький радиатор с шумным вентилятором. Скромна и комплектация: один диск с драйвами, переходник с DVI на аналог, удлинитель для TV-Out и тоненький мануал.

SAPPHIRE RADEON X800 GTO2

ядро: ATI RV480

чипсет: Radeon X800GTO

шина памяти, бит: 256

объем памяти, Мб: 256

частота ядра: 400

частота памяти: 490

тип памяти: GDDR-3

Итак, перед нами еще один вариант платы на основе чипа X800GTO от небезызвестной Sapphire. Одним из основных отличий является наличие 12-ти конвейеров против восьми, как у той же GT. Дело в том, что на данной плате не имеется аппаратной блокировки конвейеров, и с помощью обновленной версии BIOS или специальных утилит ты можешь модернизировать карту до 16-кон-

лучшая покупка
лучшая покупка
по мнению редакции

200\$

РЕЗУЛЬТАТЫ ИГРОВОГО ТЕСТИРОВАНИЯ

БЕЗ АНТИАЛАЙЗИНГА И АНИЗАТРОПНОЙ ФИЛЬТРАЦИИ

ПРИ АНТИАЛАЙЗИНГЕ И АНИЗАТРОПНОЙ ФИЛЬТРАЦИИ

1024/768 1600/1200

1024/768 1600/1200

DOOM 3

SAPPHIRE ATI RADEON X1300
MSI RX1300PRO-TD256E
SAPPHIRE ATI RADEON X800GTO2
HIS ATI RADEON X800GTO
GECUBE RADEON *800GTO
POWERCOLOR X800GT EVO
POWERCOLOR X800GT
GIGABYTE RADEON X800 (RX80256D)
SAPPHIRE RADEON X700 PRO TOXIC

119
106
87
85
81
83
80
75
71

87
82
75
72
68
66
64
61
54

88
84
78
72
71
70
67
64
60

71
69
62
57
55
55
51
47
42

HALF LIFE 2

SAPPHIRE ATI RADEON X1300
MSI RX1300PRO-TD256E
SAPPHIRE ATI RADEON X800GTO2
HIS ATI RADEON X800GTO
GECUBE RADEON *800GTO
POWERCOLOR X800GT EVO
POWERCOLOR X800GT
GIGABYTE RADEON X800 (RX80256D)
SAPPHIRE RADEON X700 PRO TOXIC

135
128
99
92
84
83
76
72
67

92
86
78
76
71
65
59
52
48

115
109
92
87
82
81
79
71
65

81
79
67
63
61
63
60
54
36

FAR CRY

SAPPHIRE ATI RADEON X1300
MSI RX1300PRO-TD256E
SAPPHIRE ATI RADEON X800GTO2
HIS ATI RADEON X800GTO
GECUBE RADEON *800GTO
POWERCOLOR X800GT EVO
POWERCOLOR X800GT
GIGABYTE RADEON X800 (RX80256D)
SAPPHIRE RADEON X700 PRO TOXIC

76
73
65
62
60
59
58
55
51

69
67
59
57
54
53
53
50
43

62
62
58
55
51
49
45
41
38

44
46
39
36
32
30
28
24
20

F.E.A.R.

SAPPHIRE ATI RADEON X1300
MSI RX1300PRO-TD256E
SAPPHIRE ATI RADEON X800GTO2
HIS ATI RADEON X800GTO
GECUBE RADEON *800GTO
POWERCOLOR X800GT EVO
POWERCOLOR X800GT
GIGABYTE RADEON X800 (RX80256D)
SAPPHIRE RADEON X700 PRO TOXIC

70
67
61
58
55
51
48
45
41

62
60
56
51
47
44
41
37
33

60
61
55
52
52
50
46
41
35

39
38
29
27
25
24
22
20
17

вейерной. Забавно. Плюс ко всему на плате установлена память GDDR-3. За такие небольшие деньги мы получаем практически вариант X800XL. Карта работает при поддержке метода компрессии 3D с технологией SmartShader и SmoothVision и обеспечивает снижение используемой полосы пропускания памяти до 25%. Из минусов отметим необходимость в дополнительном питании от БП и традиционную для Sapphire скудную комплектацию.

SAPPHIRE RADEON X1300

ядро: ATI RV515
чипсет: Radeon X1300GTO
шина памяти, бит: 256
объем памяти, Мб: 256
частота ядра: 450
частота памяти: 500
тип памяти: GDDR-3



**Выбор
редакции**
лучший продукт
по мнению редакции

210\$

Второй агрегат с графическим ядром RX1300, представленный в нашем тесте, мало отличается от подобного продукта от MSI. Бросается в глаза явное внешнее отличие от всех претендентов на чемпионство: большой кулер размером практически во всю плату, он имеет контакт практически со всеми чипами, расположенными на лицевой стороне карты. Не очень эффективное охлаждение, тем не менее, не мешает плате показывать не только хорошую производительность, но и работать без какого-либо шума. Эта плата — отличный выбор для геймеров, к тому же есть поддержка CrossFire, так что не должно быть проблем с играми, как и при выборе слота на материнской карте, потому как производитель наладил выпуск данного видеоконтроллера в двух вариантах: как для AGP(8x/4x), так и для PCI-E. В комплекте присутствует, помимо системного диска, мануала и двух переходников, еще и игровой CD. Среди минусов отметим довольно высокую цену.

GECUBE RADEON X800GTO

ядро: ATI RV480
чипсет: Radeon X800GTO
шина памяти, бит: 256
объем памяти, Мб: 256
частота ядра: 400
частота памяти: 500
тип памяти: GDDR-3



218\$

Несмотря на свой неказистый внешний вид, данное устройство весьма неплохо показало себя и при тестировании, и при разгоне. Дело в том, что в качестве системы охлаждения на карту установлена, кроме большого радиатора и практически бесшумного кулера, тепловая трубка, которая находится внутри медного ра-

диатора в форме буквы «U». Одним словом, на данной карте охлаждение обеспечивается лучше, чем на других агрегатах, если не считать, конечно, PowerColor с водянкой. Само собой, на данной плате имеется аппаратная поддержка DirectX 9, SmartShader 2.0, SmoothVision 2.1, Fullstream, а также программная — в лице Hydravision.

Кроме аналогового внешнего выхода, на торце карты можно найти DVI-порт и TV-Out. Разрешение, возможное при использовании, стандартно для всех плат такого типа: 2048x1536 при 85 Гц для VGA и 1024x768 для TV-out. Особенных минусов отмечено не было. На фоне остальных адаптеров этот продукт ничем более и не выделяется. Хороший середнячок. Цена также средняя.

GIGABYTE RADEON X800 (RX80256D)

ядро: ATI RV423
чипсет: Radeon X800
шина памяти, бит: 256
объем памяти, Мб: 256
частота ядра: 400
частота памяти: 350
тип памяти: GDDR-3

Наверное, это одна из самых слабых плат среди представленных в тесте. Несмотря на свою 12-конвейерную архитектуру и 256-разрядный интерфейс памяти GDDR3, контроллер весьма плохо справляется с поставленной перед ним задачей. Интересен тот факт, что карта является полным аналогом X850XL, и отличается только чип, который установлен на данной плате с урезанным числом конвейеров с 16 до 12-ти. Однако на саму карточку просто стоит взглянуть. Мощнейший радиатор, сквозь который проходят две тепловые трубки, сжимает плату с двух сторон, как бутерброд.

Обеспечивается потрясающее охлаждение. Комплектация Gigabyte тоже порадовала: кроме самой платы, в нее входят три диска (два игровых и один с драйверами) и симпатичный переходник, не считая стандартного с цифры на аналог, на TV-Out, который может крепиться к корпусу с помощью специальной наклейки и обладает переключателем TV/HDTV. Все хорошо, только, как мы уже писали, карточка сильно не дотягивает до остальных, да и за такую цену, возможно, стоит попробовать найти что-нибудь получше.



200\$

ИТОГО:

Для итога скажем, что все платы вели себя достойно. Большинство из них станут и радостью геймеру, и подарком оверклокеру. Если не сильно акцентировать внимание на ценах, можно смело порекомендовать любую из приведенных в тесте плат.

Награды же распределились следующим образом: за лучший результат по производительности, если не учитывать стоимость, награду «Выбор редакции» получает плата Sapphire Radeon X1300 — она стоит того. За модернизацию карты с 12-ти конвейеров до 16-ти, за потрясающие результаты при разгоне и игровом использовании, а также за небольшую при всем этом цену награду «Лучшая покупка» мы решили присудить достойнейшему видеоконтроллеру Sapphire Radeon X800 GTO2.

Технические характеристики:

ПОДДЕРЖИВАЕМЫЕ ФОРМАТЫ: CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-R, DVD-RW, DVD+RW, DVD+R, DVD+R DL, CD TEXT, CD EXTRA, CD-DA (AUDIO), CD-I, CD-ROM XA, PHOTO CD, VIDEO CD, CD-ROM, CD+G (KARAOKE CD), DVD-VIDEO, DVD+VR, DVD-VR

ВРЕМЯ ДОСТУПА: DVD-ROM: 150 мс, CD-ROM: 100 мс
СКОРОСТЬ ЧТЕНИЯ: CD-ROM: 48X; DVD-ROM: 16X
СКОРОСТЬ ЗАПИСИ: DVD+R: 16X, DVD+RW: 8X, DVD-R: 16X, DVD-RW: 4X, CD-R: 48X, CD-RW: 24X, DVD+R9 (DUAL LAYER): 4X
БУФЕР, МБ: 8
ИНТЕРФЕЙС: SERIAL ATA
РАЗМЕРЫ, ММ: 146X42X170
ВЕС, КГ: 1

Plextor PX-716SA



PLEXTOR НАРЕЖЕТ

СНОВА В НАШИ РУКИ ПОПАЛ DVD-ПРИВОД, НА ЭТОТ РАЗ ОТ КОМПАНИИ PLEXTOR. МНОГО ИХ РАЗВЕЛОСЬ В ПОСЛЕДНЕЕ ВРЕМЯ, НО МЫ РАДЫ, ИБО ЧЕМ БОЛЬШЕ ВЫБОР, ТЕМ БОЛЬШЕ ВЕРОЯТНОСТЬ ВЫБРАТЬ ДЕЙСТВИТЕЛЬНО НУЖНОЕ

Девайс Plextor PX-716SA, когда он попал к нам, был упакован в обычную картонную коробку с надписями о модели привода и используемом интерфейсе. Кстати об интерфейсе. В отличие от большинства современных приводов, данное устройство подключается через интерфейс Serial ATA, что, естественно, не может не сказаться позитивно на скорости его работы. Заглянув в коробку, мы убедились, что комплект поставки не очень богатый и ничем не отличается от OEM, но самое необходимое присутствовало. Парочка шнуров для подключения (питание и интерфейсный кабель для SATA), диск с программным обеспечением и руководством пользователя (особенно приятно, что компания Plextor не забыла перевести все и на русский язык). Кроме подробного описания на диске, есть и бумажный вариант инструкции, в которой кратко рассказано, как подключить устройство к компьютеру. В отличие от своего интерфейса, внешне этот DVD-рекордер ничем не отличается от всех своих собратьев, но это и не важно, так как модель PX-716SA является внутренней. На передней панели присутствует кнопка для автоматического выдвижения лотка и индикатор работы. Привод подключается без проблем, распознается ОС Windows XP SP2 и не требует дополнительных драйверов.

Поговорим о способностях и поведении Plextor PX-716SA в условиях эксплуатации. Для получения информации о данном приводе воспользуемся программой Nero InfoTool. Привод читает со скоростью 40X, 32X, 24X, 8X, 4X и записывает со скоростью 48X, 32X, 16X, 8X, 10X, 4X в зависимости от типа носителя. Оснащен буфером на целых 8 Мб и поддерживает практически все распространенные сейчас форматы оптических дисков.

Как же PX-716SA ведет себя в реальной ситуации? Будем оценивать его поведение с помощью программы Nero CDSpeed. Работа с диском начинается с его загрузки в лоток, который выдвигается достаточно быстро (1,7 с) и шумно, а загружается за 1,2 с. Распознавание диска происходит мгновенно.

TEST_LAB ВЫРАЖАЕТ БЛАГОДАРНОСТЬ ЗА ОБОРУДОВАНИЕ, ПРЕДОСТАВЛЕННОЕ НА ТЕСТИРОВАНИЕ, КОМПАНИИ «НИКС — КОМПЬЮТЕРНЫЙ СУПЕРМАРКЕТ»

Мы попробовали оценить и скорости устройства на различных дисках, причем они будут отличаться не только форматами, но и своим состоянием. Сначала обычный диск формата CD-R, абсолютно чистый и новый. Скорость записи, показанная программой, составила 30,44X (среднее значение), скорость чтения — 32,22X (среднее значение), при этом загрузка CPU — 0%, 1%, 2%, 4% соответственно скоростям 1X, 2X, 4X, 8X, что довольно мало. Далее мы испытали девайс на чтение-запись болванок CD-RW. Экземпляр, который использовался в тесте, бывал в боях, но остался жив и имел лишь незначительные царапины. Здесь скорость стабильно держалась 10,00X в течение всего цикла записи, скорость чтения составила 32,35X (среднее значение). Если скорости такие, значит, привод не боится царапин. CPU при работе с CD-RW был загружен так же, как и в предыдущем случае. И наконец, диск DVD-формата, сильно заляпанный и прилично поцарапанный, скорость чтения этого убитого носителя сильно колебалась и в среднем составила 9,12X. Однако главное — то, что привод прочел диск целиком. Снимаем шляпу перед ним.

DVD-привод достаточно приличный, об этом свидетельствуют хорошие скорости записи-чтения, отсутствие ошибок, быстрое распознавание дисков и малая загрузка CPU, однако вибрация, шумность работы и нагрев бывают и от них никуда не деться. Правда, эти результаты PX-716SA сравнимы с показателями обычного привода, как разница между дорогим спортивным автомобилем и российской «десятой». Цена соответствующая — \$135

Тест на чтение убитого DVD выдержал с честью — дошел до конца



е-мыло

SPEC@REAL.HAKER.RU

КАЖДЫЙ РАЗ Я С ТРЕПЕТОМ И РАДОСТЬЮ РАЗГРЕБАЮ КУЧИ СПАМА, ПРИХОДЩИЕ НА НАШ РЕДАКЦИОННЫЙ ЯЩИК, НАХОЖУ В НИХ ЖЕМЧУЖИНЫ, КОТОРЫЕ МНОГИЕ ИЗ ВАС НЕ ЛЕНЯТСЯ НАМ ПИСАТЬ. СПАСИБО! ВОИСТИНУ, ВЫ НЕ ДАЕТЕ НАМ ПОЧУВСТВОВАТЬ СЕБЯ ЗАБЫТЫМИ! | НА ПИСЬМА ОТВЕЧАЛ SKYWRITER

ОТ: Юлия [julianovo@mail.ru]

ТЕМА: Где мой сюрприз?

Здоровья и процветания!

Я далеко не хакер. Скорее, все-таки, чайник.

Но и свой «сюрприз» (из «Спец Хакера» N 09(58), сентябрь 2005)

упускать не хочется.

SMS отправила и уже полдня жду ответа. А ответа нету!

Может, еще не все потеряно?

С наилучшими пожеланиями, <censored> Юлия.

ОТВЕТ: И тебе не хворать, Юлия!

Дело в том, что с сюрпризом у нас все надежно: ребята действительно отвечают за доставку SMS, не зря они берут такие зверские деньги. Обычно проблема доставки SMS заключается не в этих ребятах, а в твоём операторе, который не поддерживает такие услуги и не позволяет тебе заказывать любые мелодии, картинки и т.п. стафф. Такое частенько встречается среди тех, кто находится за пределами великой и необъятной Родины журнала «Хакер Спец» — Россия. Методов борьбы, к сожалению, придумано не было ;-).

Люби и уважения,
твои Спецы!

ОТ: Юрий <censored> [uriy@holdpaq.ru]

ТЕМА: Тематический выпуск! Срочно!

Доброго времени суток, уважаемая редакция!

Вот такая ситуация... Написал я книгу о полезных программах, в нее входят вот такие главы:

- О КНИГЕ: О ЧЕМ И ДЛЯ КОГО;
- КАКИЕ БЫВАЮТ ПРОГРАММЫ;
- КТО И КАК ДЕЛАЕТ ПРОГРАММЫ;
- СОФТ-КАТАЛОГИ РУНЕТА;
- ОБЗОР АРХИВАТОРА WINRAR;
- ОБЗОР ПРОГРАММЫ FLASHGET;
- ОБЗОР ПРОГРАММЫ REGEX DELUXE;
- ОБЗОР ПРОГРАММЫ WEBMONEY;
- ОБЗОР ПРОГРАММЫ ICQ;
- ОБЗОР ПРОГРАММЫ AD-AWARE SE;
- ПОДРОБНЕЕ ВО ВЛОЖЕНИИ...

Состоит она из 251-го word-листка, включая иллюстрации (329 345 знаков без пробелов). В издательстве ее не приняли, обосновав:

1 ТЕКСТ В НЕКОТОРЫХ МЕСТАХ СХОЖ С ТЕМ, КОТОРЫЙ

В haker.ru (ЭТО Я СВОИМИ СЛОВАМИ ГОВОРЮ В ОБЩЕМ О ТОМ, ЧТО ОНИ СКАЗАЛИ).

2 ПРИЧЕМ ТУТ WINRAR, ЕСЛИ ДРУГИЕ ПРОГРАММЫ ОБ ИНТЕРНЕТЕ :)?

3 МАЛОВАТО, МОЛ, ОПИСАННЫХ ПРОГРАММ...

Вот что хотел предложить: можно ли как-нибудь протолкнуть эти статьи в ваш журнал? Можно было бы, например, сделать что-то типа тематического выпуска!? Или что-то в этом роде... Образец какой-нибудь статьи могу прислать... Я думаю, получится неплохой выпуск, т.к. программы пользуются популярностью и многим будет интересно почитать этот выпуск... Да и по толщине он приличный будет :). Все статьи эксклюзивные, рассмотрены последние версии программ...

Что вы можете предложить? Есть какие-нибудь идеи?

Также интересует вопрос о гонораре :)...

С нетерпением жду ответа!..

ОТВЕТ: Здравствуй, Юрий!

Жил-был некий автор, который очень любил жать клавиши. Жал он их и жал, пока не сказал ему Господь наш, что графоманство — грех. И перестал автор жать клавиши, и воцарился мир и порядок на Земле. Но ты, видимо, скажешь, что я отвечаю не в тему ;-). Что ж, хорошо. Отвечу в тему.

Данные статьи, описывающие ПО безусловно хакерского характера, вполне можно протолкнуть в наш журнал! У нас даже есть специальная форма отношений с теми, кто хочет проPR'ить что-то через Спец. Форма описана достаточно подробно по адресу www.glc.ru/post/15002/default.asp?mg=xs. Это как раз страница с гонорарами.

Если лень сходить на эту страничку, то коротко ознакомься с расценками на полосы: одна полоса в журнале стоит \$7000, Спец занимает 105 полос, итого 7000x105 = \$735 000. Именно во столько тебе обойдется публикация твоих статей в полный номер, если, конечно, наш рекламный отдел согласится ;-). С терпением и пониманием ответили.

ОТ: валера моисеенко [valik05@inbox.ru]

ТЕМА: Взлом!

Здравствуйте! Я большой поклонник вашего журнала.

Меня интересует взлом. Я хотел бы узнать, как можно взломать сайт или форум. Подскажите мне, пожалуйста!

ОТВЕТ: Aloha! Валерий, взломать форум или сайт элементарно! Необходимо определить, на каком компьютере установлен web-сервер (о том, что такое web-сервер, ты можешь узнать из обширной литературы соответствующей тематики), взять лом/топор (подойдет любой тяжелый металлический предмет) и отправиться к серверу. Далее хорошенько размахнуться и... С треском и звоном ты взломаешь форум или сайт. Удачи!

P.S. А вообще — RTFM. О значении этой аббревиатуры также можно узнать из специализированной литературы и ресурсов Internet ;-).

ОТ: matthew [matthew@dvru.ru]

ТЕМА: ХЕЛП ПЛИЗ

Здравствуйте, спес.
Дорогой журнал! СПАСАЙ!!!!
Я хочу сделать жучок.

1 Я КУПИЛ ГЕТИНАКС, НО УМА НЕ ПРИЛОЖУ, КАК НА ЭТОМ ЗОЛОТИСТОМ КУСКЕ ВЫРЕЗАТЬ ДОРОЖКИ.

2 В МАГАЗИНЕ НЕ БЫЛО ТРАНЗИСТОРА КТ386А9 — ЧТО ДЕЛАТЬ, НА ЧТО ЗАМЕНИТЬ?

3 МЕНЯ СПРАШИВАЛИ МОЩНОСТЬ РЕЗИСТОРОВ — Я НЕ ЗНАЛ, КАКУЮ БРАТЬ.

4 КАК ОТЛИЧАТЬ ВСЕ ШТУКИ, КОТОРЫЕ МНЕ ДАЛИ? ЧТО ЗНАЧАТ ПОЛОСКИ И ЦИФРЫ? ОБЪЯСНИТЕ, ПЛЗ.

И как выглядит печатная плата жучка на странице 37? ПОМОГИТЕ, ПРОШУ!!!!

ОТВЕТ: Привет, Матвей!

Что я могу тебе посоветовать... Тут очень сложно решить даже, с чего и начать. Советую тебе прочитать наш журнал, то есть Спец, с его самых первых номеров — с тех пор и существовала рубрика «Паяльник». Именно эти описания помогают, как правильно работать с этим самым «золотистым куском», как проверять транзисторы, как искать замену им. В общем, многое-многое, что бы очень помогло тебе. Помимо этого, советую обратиться в местную библиотеку или книжный магазин с запросом на книжки для начинающих радиолюбителей. В общем и целом могу пообещать, что, до тех пор пока ты что-то не соберешь, ты постоянно будешь завален тяжелой работой. Однако оно того стоит: у тебя будет жучок ;-).

В общем, усваиваем 11-ю заповедь — RTFM :-).

Творческих успехов!

ОТ: Дмитрий Артюхин [lianozov@bk.ru]

ТЕМА: Сюрприз в Журнале «Хакер», то есть на диске

Какой пароль? => На диске в выпуске за этот месяц есть файл surpriz.rar — зашифрованный (подскажите пароль). Я юзал-юзал и пришел к выводу о том, что я ламер =)).

ОТВЕТ: Честно говоря, я бродил по офису грустный и у каждого, кого встречал, спрашивал пароль, но, к сожалению, все уже давным-давно забыли его :-). Уж больно они у нас сложные. Так что единственный способ — отправить SMS :-). Впрочем, вру!

Есть еще один способ под названием «Китайская лотерея». Сущность лотереи в следующем. В каждый китайский телевизор встраивается чип, который под-

бирает пароль к архиву с диска. Когда пароль подобран успешно, на экран выводится надпись: «Позвоните по телефону <ТВОЙ-ТЕЛЕФОН> и сообщите следующую строчку для получения выигрыша: ПОДОБРАННЫЙ-ПАРОЛЬ». Учитывая количество китайцев и тот факт, что у каждого десятого из них есть телевизор, предположим, что пароль подберется где-то за пару дней :-).

Сообщи о результате!

Ждем, твоя редакция.

ОТ: Елена Ляйрих [cni@elsu.ru]

ТЕМА: Уважаемая редакция!

Уважаемая редакция! Я являюсь Вашим постоянным читателем с 2003 года, причем подписываюсь на него, а не покупаю. Хочу выразить Вам свое недоумение по одному вопросу (хотелось бы верить, что вы делаете это не нарочно). Ваш журнал ориентируется исключительно на мужскую аудиторию. Вам, наверное, и невдомек, что существует еще одна половина человечества, у которой, кроме прелестей тела, есть еще и мозг и которой интересно читать Ваш замечательный журнал. Поверьте, нас не так уж и мало. Неверный ход, ребята. Не теряйте эту, пусть и не очень большую, часть аудитории. Недоумение мое по поводу Вашего отношения к женскому полу вызвала анкета в #10(59), в которой присутствовала графа «Твое семейное положение» с вариантами ответов только для мужчин. А если я замужем? Да и в интернете Ваша аудитория определена как исключительно мужская. История «женского вопроса» в ИТ еще совсем не исследована. О себе: Елена, 36 лет, высшее филологическое образование, замужем, работаю в государственном университете. С уважением, спасибо за замечательный журнал.

ОТВЕТ: Не менее уважаемая Елена!

Очень рады, что обрели еще одного читателя из «еще одной половины человечества», и, безусловно, не хотим отказываться от него — будем холить и лелеять Вас под своим крылом. Однако, несмотря на то, что у нас достаточно много читательниц, их все же намного меньше, чем читателей. Увы. Видимо, именно поэтому журнал ориентирован на «мужскую» аудиторию.

Тем не менее, я практически всей своей джентльменской честью клянусь приложить все усилия, чтобы свергнуть патриархат и таки восстановить справедливость (в том числе исправление анкеты)!

С уважением,

Спец.

ОТ: Александр [s184@mail.ru]

ТЕМА: Е-мыло

Здравствуйте, господа.
Подскажите, пожалуйста, если знаете, название программы, которая вычисляет пароль перебором вариантов и их посылкой в буфер клавиатуры. Спасибо за внимание.

ОТВЕТ: Здравствуйте, гражданин.

Таких программ целая толпа, но сама быстрая и надежная — это собственные усилия. Нужно лишь сесть перед компьютером и нажать «а», потом <Enter>. Если не подошло, нажать «b» и <Enter> и т.д. В общем, если приносиваться и набирать в среднем один символ в 0,2 с (около 300 символов в минуту, да ?;-)), то восьмизначный пароль из циферок и буквочек ты подберешь, по скромным оценкам, за 1,5 млн. лет. Не так уж и плохо :-).



НОЧНАЯ РАБОТА

STORY

NIRO (NIRO@REAL.XAKEP.RU)

Тушина уже очень давно не вызывали среди ночи — так давно, что он напрочь позабыл, на что похож трезвон телефона в квартире после полуночи. Досматривая пятый или шестой сон, из глубин объятий Морфея он с непониманием вслушивался в непонятный звук, появившийся из ниоткуда. Громкий, настойчивый звук тащил Тушина из-под одеяла в сторону прикроватной тумбочки против его воли, где-то внутри его еще жил врач «Скорой помощи», отпахавший свои одиннадцать лет в реанимационной кардибригаде. И как ни хотелось зарыться под подушку, как ни хотелось продолжать смотреть сон, в котором школьные друзья вперемешку с коллегами посреди незнакомого леса жарили шашлык, пришлось открыть глаза и протянуть руку...

«Не дай бог ошиблись номером», — подумал он, пристраивая локоть на подушку.

— Да... Да, это я.

В трубке звучал взволнованный голос Венечки Смирнова:

— Петр Михайлович, вы должны приехать... Это... Я не возьму на себя ответственность...

— Криминал? — сонно спросил Трушин, отметив про себя, что Вениамин даже не извинился за столь поздний (или уже ранний?) звонок. — Ты там что, один?

— Так получилось, Петр Михалыч... Я отпустил лаборантку, у нее сегодня у сына юбилей, двадцать лет. Она так просила, что я не смог отказать. И теперь...

— Так, стоп, — прервал тираду Тушин. — Смирнов, ты пока еще представляешь, кому ты звонишь?

— Да, — коротко выдохнул на том конце провода Венечка. — Вы думаете, это так просто было взять и ваш номер набрать в полвторого ночи? Я тут вокруг телефона уже полчаса хожу и сам себя уговариваю.

«Так... Полвторого. Хоть время узнал».

— Ты можешь толком рассказать, зачем я тебе понадобился?

— Вы решите, что я пьян, Петр Михалыч. Или еще что-нибудь. Я вам вызову такси и сам заплачу, только вы приезжайте, пожалуйста, потому что они тут не уходят, а я просто боюсь... Дальше лезть...

— Они? Кто такие «они»? — переспросил Тушин, уже угадывая ответ.

— Милиция. Вы же сразу сказали — «криминал».

— Я не сказал, я спросил. Это разные вещи. В общем, поверю на слово, что ты так просто среди ночи мне бы не позвонил. Такси не надо, сам доберусь, у меня машина во дворе.

Тушин положил трубку, сел на кровати, нащупал тапочки. Что там за чертовщина у Смирнова?

Встав, он прошел в ванную, залез под душ, поддал холодной, чтобы быстрее проснуться. Мышцы под кожей заходили ходуном, пытаясь дрожью спасти Тушина от ледяных струй. Он выдержал всего минуту, потом выскочил из-за полиэтиленовой шторки и принялся энергично растираться. Сон как рукой сняло, осталась только усталость, ощущение того, что не отдохнул как следует, сон не досмотрел...

Иногда он вспоминал свои «скоромощные» будни, четко помнил, что после трех часов ночи не испытывал к больным ничего, кроме раздражения, которое плохо скрывал. Люди, вызывавшие его в такое время, обычно болели давно и тяжело, но почему-то считали, что самое главное — это пережить ночь, дожидаться утра и вот уже тогда... Но практически никто с ночами не справлялся: ни сердечники, ни больные животы, ни почечные колики. Приходилось наряду с уколами анальгетиков и таблетками нитроглицерина читать унылые злые лекции на тему «Где вы были раньше?» Люди частенько обижались, несколько реже извинялись, но ответа на свой вопрос Тушин за все годы работы так и не добился. Пожатие плеч, разговоры типа «Я думал, пройдет» или «Да не хотелось вас беспокоить...» его раздражали. Кого же еще беспокоить, если не «Скорую помощь»? Пожарников, что ли?

Вот и сегодня к нему вернулось давно забытое чувство: «Кого там еще принесло на ночь глядя?» Правда, помощи просил его коллега, подчиненный, это накладывало определенные обязательства. В таких случаях нужно молча идти и делать свое дело, беря часть ответственности или всю на свои плечи. Вполне возможно, что мнение Тушина окажется последней инстанцией, которая снимет все возникшие вопросы. Иногда было достаточно только его имени и авторитета. Из головы не выходило то, что Смирнов даже не стал ничего объяснять по телефону — он просто поставил Тушина перед фактом. Дело, по мнению Венечки, того стоило.

Петр Михайлович оделся, вышел во двор. «Ракушка» стояла прямо напротив подъезда, желать более удачного расположения гаража было трудно. Металлическая дверца лягнула, складываясь, из темноты показался капот его «Ауди».

Машина мягко выехала из гаража. Тушин, продолжая рассуждать про себя о том, что же могло случиться, сел за руль и направился к своему месту работы, где его ждал Венечка Смирнов.

В пути он долго размышлял о том, по каким причинам решил сменить свою работу, такую беспокойную и нужную, нужную до слез, до криков и мольбы профессию врача скорой помощи, на... Как бы это помягче выразиться...

— Да говори уже прямо, — вслух сказал Тушин. — Надоело тебе слушать все эти крики и видеть все эти слезы. Надоело. Хотя неужели на новом месте этих слез стало меньше?

По сути дела, ответ был положительный. Меньше. Реально меньше. Да и эти слезы были какими-то уравновешенными, что ли. Сам Тушин старался не замечать их, считая все это издержками профессии, к людям не выходил, ничего никогда не рассказывал, решаясь на разговоры только в крайних случаях. Для этого у него были подчиненные, которые умели хорошо и складно объяснять, что да как.

Петр Михайлович аккуратно вел машину по ярко освещенным улицам ночного города и вспоминал свою молодость на «Скорой». Вспоминал коллег, фельдшеров, водителей. Он помнил каждую машину, на которой совершал свои выезды сутки через трое, а иногда и чаще. Он и сейчас мог найти такие районы города, о которых имели довольно слабое представление даже таксисты. Помнил каждую смерть и каждого спасенного... Хотя вряд ли — скорее всего, он лукавил. Невозможно помнить столько людей, которых ты доставил в центральную клиническую больницу, ногами открывая дверь в приемное отделение. Невозможно помнить свое кладбище, можно только вспоминать отдельные холмики на нем, отметки о прожитых годах. Они пили почти всегда молча, умалчивая о том, о чем думали, хотя их вечеринки порой бывали крайне шумными, пока кто-нибудь не начинал говорить о работе. И тогда чья-нибудь жена тихо кивала таким же, как она, — терпеливо ждущим, когда все кончится. И все мирно кончалось, все расплазались по своим норам до следующей смены.

Но в какой-то момент все сломалось и покатило к черту. Тушин вдруг понял, что в его душе не осталось ничего, кроме цинизма и наплевательского отношения к смерти. Ничего, что могло бы удержать его от морального разложения. Несколько раз он достаточно равнодушно провозжал в последний путь людей прямо на носилках внутри машины, а потом узнавал, что они чьи-то родственники, знакомые, друзья. Его это перестало задевать так, как задевало раньше в институте, а потом в первые годы работы.

И он ушел. Ушел, удивив всех своих коллег, мало кто другой решался на такой поступок. Ушел, сидел полгода дома, осмысливая свой внутренний статус. Жена молчала, терпеливо ожидая, когда к ее грошовой зарплате учителя добавится хоть что-то. И когда это «что-то» добавилось, собрала вещи и ушла к матери.

Конечно же, он нашел работу. Конечно же, он не смог уйти из медицины. Просто медицина бывает разная. Жена не поняла.

Он ушел из мира живых. Он стал патологоанатомом. Ему удалось возглавить патологоанатомическое бюро, правда, опыта работы у него было немного, но должность была больше административная, хозяйственная. Он пошел на нее едва ли не с радостью — так ему претило видеть сам процесс умирания, что он был готов оказаться по любую его сторону. Выбрал сторону смерти. Он был не в состоянии продуктивно общаться с живыми, не было ни желания для этого, ни терпения. Бессмыслица получалась. Он даже не мог толком проконсультировать соседей по подъезду: они раздражали его, как раздражает пяточная шпора. Глупо, больно, но ничего не поделаешь.

В мире смерти все оказалось проще, люди плакали меньше. Он погружился в пучину свидетельств о смерти, хозяйственную волокиту, ремонт холодильников, работу со студентами, отдавшими себя судебной медицине. Сам понемногу читал специальную литературу, пытался вскрывать,

благо Бог не обидел силой. Вначале под руководством опытных коллег, потом сам — что попроще. Про себя называл свое бюро, ставшее ему вторым домом, «Бюро грустных услуг». По городу как грибы после дождя разползались всякие «Валькирии», «Тихие обители», «Обелиски» — Тушин не хотел опускаться до подобного уровня. Никаких названий. Никаких акционерных обществ. «Нельзя наживаться на смерти» — в этой фразе есть два слова, которые не могут существовать вместе. Он закрывал глаза на то, что его товарищи по работе берут деньги. Сам не брал. Во-первых, он не был профессионалом, а следовательно, мог взять деньги за ошибку. Во-вторых, смотри выше.

Иногда он задумывался, есть ли на свете причина, которая заставила бы его принять деньги за свою работу. Болезнь близких; безвыходное положение вроде пожара — унесло все, что ты нажил; банально вдруг проснулась человеческая корысть. Факторов было много, но ни один не возникал в жизни Тушина. Он тащил на себе «Бюро грустных услуг» за обыкновенную зарплату, чем снижал небывалое уважение к себе. Одни врачи помогали ему на вскрытиях, другие втихую исправляли его ляпсусы в надиктованных протоколах, третьи просто не забывали угостить его чашкой кофе. Уважали его все. Не все понимали...

Дорога стала практически пустынной, скучной и однообразной. Тушин включил радио, пытался вслушаться в трепотню неспящих диджеев: разговор у них явно не клеился, чьи-то телефонные звонки все время обрывались, они нервничали, пытались шутить, причем пару раз довольно удачно, но на общем фоне Тушин даже не улыбнулся. Они словно чувствовали, что сейчас их слушает человек, который едет на встречу со смертью, пусть не со своей... Петр Михайлович покачал головой. Не хватало только дождика для полного счастья, чтобы ветер кидал листья пригоршнями в лобовое стекло и они прилипали бы, и только «дворники» были в силах сгрести их вбок, расшвыривая на дорогу.

Конечно же, дождь пошел. Несильный, еле заметный. В свете фар встречных автомобилей Тушин вдруг заметил, что стекла машины засверкали мелкими точками. Он хмыкнул сам себе, поздравляя за прозорливость, потом прикрыл маленькую щель в окне двери, через которую хотел покурить, включил печку. Спустил минуту вспомнил, что так и не разобрался с режимами обогрева: постоянно путаясь в клавишах кондиционера, он опять включил что-то не то, окна стремительно покрывались туманом, настолько плотным, что он машинально протянул руку перед собой и протер ладонью лобовое стекло. В получившийся квадратик он с трудом различал, что же происходит на дороге.

Мелькнули сбоку и пропали где-то вдаль красные габариты обогнавшей его машины. Брызнул в глаза светоотражатель на знаке «Крутой поворот». Пронесли мимо несколько полосатых столбиков и длинный отбойник вдоль какого-то забора из красного кирпича. Знакомые ориентиры были сейчас размыты, появлялись внезапно нечеткими и так же внезапно исчезали. Тушин немного занервничал, напрягся. Руки на руле быстро остоптели. Всплыла мысль о том, что уже давно пора сбросить скорость, остановиться, взять тряпку из кармана на двери и, как нормальный человек...

Из темноты вырос, как исполинский гриб, стоящий на обочине «дальнобойщик», не обозначенный огнями. Водитель, остановившийся на ночь в отсутствие кемпинга. Машина, в десять раз выше и в сто раз тяжелее «Ауди». Контейнер, не помещившийся целиком на обочине, выпирал на трассу, как грыжа.

Тушин едва успел увидеть отблеск, отразившийся от габаритного огня. Он рванул рулем так, как уворачиваются от летящего камня: сам наклонился за рулем, будто пытался спрятаться за приборную доску.

Машина была послушна, проявила все качества, присущие высшему европейскому классу. Занос был коротким, покрышки слегка взвизгнули на влажной, еще не основательно намочшей дороге. Перед глазами промелькнули штрихи разделительной полосы, очередная порция листвы метну-

« ПО-
немногу чи-
тал специ-
альную лите-
ратуру, пы-
тался вскры-
вать »

« Смотри, червячки свежие... На рыбалку не собираешься? »»

лась на капот. Каким-то десятым чувством поняв, что от удара он ушел, Тушин дал по тормозам, даже не пытаясь вернуть машину на прежнюю траекторию. Его кинуло на руль. Все, чего он ждал в это мгновение, — когда же она остановится. Он был бы рад чему угодно: пусть она уткнется в ограничительный столбик, пусть скатится в кювет, пусть это будет дерево или дорожный знак. Просто пусть она остановится...

Тормозной путь был длинным. «Ауди» ушла далеко на полосу встречного движения, скособочившись от торможения с незначительным заносом. В полосу, освещенную фарами, попала противоположная обочина с порванной покрывкой на ней.

— Сто-о-ой! — закричал Тушин и потянул на себя руль, как штурвал самолета. И машина, бросив вперед из-под заблокированных намертво передних колес кубометр земли, замерла. Тишина длилась всего секунду. Ошалевший от происшедшего Тушин с трудом приходил в себя, чувствуя, как слабеют руки и начинается жуткое сердцебиение. Он отшатнулся от руля, как будто тот был покрыт копошащимися гусеницами, — с отвращением и испугом. Отодвинулся назад, позабыв, что у машины есть двери.

Потом он закричал. Это была жуткая смесь мата и простого крика, мольбы о помощи и проклятия. Ударив несколько раз по рулю и вызвав из недр машины длинный гудок, он наконец-то вспомнил, кто всему виной. И тогда он вышел из машины.

Все, что случилось потом, он запомнил на всю жизнь.

Навсегда.

Внезапно налетевший порыв ветра был так силен, что Тушин едва не вывихнул себе плечо, пытаясь удержать открытую дверцу. Пыль, дождевые капли, листва, мусорные пакеты, — все это взвилось с обочины, закручиваясь в маленький приземленный смерч. Петра Михайловича качнуло вместе с машиной, которая, как парус, откликнулась на ветер жуткими вибрациями. Воздушная масса, будто живая, пересекла дорогу, оставаясь видимой из-за бликов фар «Ауди» на мокрой листве. Смерч ударил в подножие исполинского тополя метрах в ста — ста пятидесяти от Тушина дальше по трассе.

И огромное, просто гигантское дерево, неожиданно качнувшись, упало поперек дороги, разломившись при ударе пополам, пышные ветви тополя вздрогнули, наполовину обронив листву.

Петр Михайлович не мог произнести ни слова. Он обернулся в ту сторону, где стоял трейлер, заставивший его затормозить, чтобы понять, видел ли водитель все случившееся, и обомлел: ОБОЧИНА БЫЛА ПУСТА. «Дальнობойщика» нигде не было.

Он явно не мог исчезнуть так быстро, большегрузная машина с огромным контейнером. Не мог — и все. И тем не менее его не было...

Венечка Смирнов всегда подавал надежды — всю жизнь, сколько себя знал. Для него «подавать надежды» означало то же самое, что для какого-нибудь ученика сантехника «подавать ключи». Его надеждами питался не он сам, а те, кто его окружал, — коллеги и соратники.

В его тусклом свете молодого дарования выросли и ушли в большую жизнь уже несколько достаточно крупных бездельников, против которых оказался бессилён Тушин с его чистой душой, не способной к конфликтам с бездарностью. Он же сам продолжал оставаться для заведующего светом в окошке, оказавшись не способным к написанию даже самой обычной кандидатской.

Работая как вол, он наравне с Тушиным тащил все, что только можно, ковыряясь в дерьме, приставляя отрубленные головы к телам, разыскивая на истлевшей одежде следы от ножа и пули, — и так уже четыре года после института. Закончив с отличием и получив «красный диплом», он, сам того не ожидая, оказался там, где был и по сей день. Многие считали его просто дурачком — для него же быть с самим Тушиным означало добиться в этой жизни практически всего. Авторитет начальства был высок, и хотя Вениамин до-

вольно быстро понял, что хотя Тушин как судебник и патологоанатом еще далек от совершенства, человеческие качества у него всегда на высоте.

Смирнов знал, что за глаза их с Тушиным называли «Чай вдвоем»: они час-тенко задерживались на работе допоздна за чашкой чая (практически никогда за

рюмкой горячительного). Одному из них было некуда спешить УЖЕ, другому — ЕЩЕ. Венечка не обзавелся семьей в свои двадцать шесть лет, с большим трудом представлял себе, как будет знакомиться со своей будущей женой. «А чем вы занимаетесь?» — «Да так, трупы вскрываю...» Тушин много раз пытался переубедить его в том, что обязательно найдется кто-то, кто будет дьявольски заинтересован этой профессией (при этом не забывая о собственной жене — полной противоположности данных заверений). Смирнов выслушивал его внимательно, как отца, потом наливал еще чаю, доставал из вазочки конфету и погружался в свои мысли.

И никто, даже его самый проницательный друг Петр Михайлович Тушин, понятия не имел, что творится в голове у молодого специалиста. А Венечка Смирнов думал об удаче.

О синей птице.

И мечталось ему совершить какое-нибудь открытие, которое перевернет все взгляды в медицине: на жизнь, на смерть, на строение человека, на его мысли и чувства. Это должно было быть такое открытие, за которое не обязательно давать Нобелевскую премию, но пусть запомнят Венечку Смирнова В ВЕКХАХ. Вот такой он был корыстный в своих мыслях.

А потом вновь начиналась работа, и он погружался в нее с головой, забывая об открытиях и врачебных подвигах — просто у каждого из нас есть своя мечта, и в краткие моменты отдыха Смирнов предавался этим достаточно безобидным мыслям.

Сегодня его мечта была готова материализоваться.

Когда он пришел на работу в ночную смену, он еще и понятия не имел о том, что работа, которая свалится на голову сегодня, будет необычной. Все как всегда: он зашел в раздевалку, сменил свой строгий костюм на халат, проверил в кармане перчатки и «Паркер», мазнул под носом ароматизатором и вышел в секционный зал.

Работа в тот момент стояла. Прямо перед носом — пара тел на катаках из морга городской больницы. Инфаркты. Фигня. Перевел глаза направо: в углу черный мешок с «молнией». На нем — только маркировка с места обнаружения. Значит, еще не тронули. Жаль, почему-то именно сегодня не хотелось быть «рыбаком».

Уходящий с дневной смены Бобровский подошел, похлопал по плечу:

— Смотри, червячки свежие... На рыбалку не собираешься? — и, рассмеявшись, направился в раздевалку. Смирнов попытался улыбнуться, это плохо получилось.

— Ну, в порядке поступления или как? — спросил он себя. — Может, есть какие-то личные пристрастия?

Пристрастий не оказалось. Заглянул в журнал, отметил, кто в каком порядке поступал. Пара санитаров перекинули деда с ближайшей каталки на секционный стол, подложили под шею и плечи деревянный брус. Голова трупа глухо стукнулась о каменную столешницу.

Лаборантка заняла свое место за столом, положив перед собой фотоаппарат и несколько пустых майонезных баночек. Смирнов коротко кивнул и принялся диктовать ей — все по протоколу.

Спустя минут двадцать, может, двадцать пять, когда выпотрошенное сердце было взвешено на весах и разрезано, когда участок некроза в нем был выявлен и диагноз подтвержден, когда оставалось только зашить тело, дверь в секционный зал внезапно распахнулась.

Ее открыли пинком ноги.

Венечка машинально поднял руки, как хирург за операционным столом, которого отвлекли от работы непрошенные гости. В зал стремительно

ворвались несколько человек в милицейской форме. В пяти шагах от двери они замерли, оглядываясь.

Вспомнился старый анекдот: «Приходит мужик на работу, а там — гора трупов!.. — А кто убийца? — Да никто: мужик в морге работал...» Хотя в общем-то Венечке было не до смеха.

Вошедшие слегка опешили от того, что увидели: двое последних даже сделали несколько шагов назад. Но потом кто-то, кто еще оставался в коридоре, громко скомандовал неразборчиво, но внушительно. Все расступились, и еще четыре человека в форме внесли в зал носилки с... (Венечка ни секунды в этом не сомневался) трупом своего коллеги.

Все трупы, конечно же, выглядят по-разному. В зависимости от того, где, как и когда умирал тот или иной человек. Но то, что все они МЕРТВЫ, нельзя не узнать. Живой человек, даже находящийся в крайней степени терминального состояния, никогда не выглядит подобным образом — неестественно.

И Смирнов понял, что предстоит внеочередная работа. Он вопросительно развел руки, словно спрашивая у всей этой милицейской братии: «Что, собственно, происходит?» На его немой вопрос быстро ответили.

Чеканным шагом, замыкая странную процессию, в зал вошел человек с большими звездами на плечах. Венечка, за всю свою жизнь не запомнивший даже вид погонов рядового, с трудом мог представить, кого в столь поздний час занесло к нему в морг, но сам вид этих звезд парализовал его волю. Пусть на какое-то время, но Смирнов полностью выпал из жизни, застыв с разведенными руками, как Будда, и разглядывая красные лампасы, которые притягивали его взгляд, словно магнит. Тем временем человек, оглядев зал, посмотрел на то тело, которое лежало перед Вениамином. Кашлянул куда-то в сторону, прикрыв рот кулаком, и сказал:

— Долго еще?

— Да... В принципе... Минут десять. Вот... Зашиваю.

— Подождем, — он снова кашлянул и медленно отошел назад на несколько шагов. — Перекур, — кинул он за спину. Потом хмыкнул и добавил:

— Кто не курит, может опривиться.

Венечка проводил взглядом тех, кто с позволения начальства рванул на улицу, пожал плечами и принялся зашивать тело. Он хоть и волновался, но дело делал быстро и аккуратно. Лаборантка заканчивала протокол, делала надписи на баночках с макропрепаратами и надеялась на честное слово доктора, который пообещал ей короткий рабочий день: у ее сына был сегодня торжественный день, двадцатилетие, она собиралась пробежаться по магазинам и приготовить праздничный обед.

Пальцы, прижимавшие к кусочку мешковины толстую слегка закругленную иглу, немного подрагивали. Пару раз Венечка ронял иголку, неловко нагибался вниз, стараясь разглядеть ее на кафельном полу в переплетении теней, и чувствовал на себе тяжелый взгляд офицера (что-то внутри нащепывало ему, что это по меньшей мере генерал, но вот в каком конкретно звании?). Офицер курил медленно, уравновешенно, словно всю свою жизнь провел в окружении мертвецов и формалина. Изредка он бросал взгляды на стены, где Венечка когда-то развесил разного рода репродукции «из жизни» нечисти, вампиров и подобной им оккультной чепухи. Все, кто работал с ним в морге, давно к этому привыкли. Похоже, что и генерал делал это с искренним любопытством, не выказывая и тени неприязни.

— Хм... — офицер издал неопределенный звук, стоя около большого плаката с изображением Дракулы. На плакате был изображен кадр из «Ван Хельсинга» — ничего особенно выдающегося. Генерал выдохнул дым прямо в дьявольскую физиономию вампира и медленно прошел вдоль стены дальше.

Венечка сделал еще несколько стежков, подтягивая нитку всякий раз, когда видел, что разрез немного расходится. Труп на столе приобретал более-менее человеческие очертания...

— А это? — генерал ткнул окурком в плакат с кадром из того же фильма, на плакате был изображен Франкенштейн. — Что за чертовщина?

Вопрос, судя по всему, растворился в пустоте. Из двоих оставшихся в помещении людей в форме один явно был не готов к вопросу и смутился; сделал вид, что ему здесь не по себе, он медленно вышел в дверь у себя за спиной и пропал. Второй же наоборот спокойно приблизился к начальству, протиснувшись между довольно упитанным генералом и столом с телом на нем.

— Франкенштейн, товарищ генерал-майор! — бодро прокомментировал он увиденное на картинке. «Генерал-майор...» — отметил про себя Венечка. — Чудовище-человек, собранный по кусочкам...

— Примитивно вы описываете, — внезапно сказал Вениамин, сам не ожидая от себя подобной смелости. Генерал обернулся к нему и пристально посмотрел в глаза.

— Как умеет, — защитил он своего подчиненного. — Мне и этого достаточно...

— Понимаю, — коротко кивнул Венечка и подумал: «Зачем я влез? Хрен с ним, с Франкенштейном... Чего они приволокли-то?» Продолжая зашивать, он принялся разглядывать то, что мог увидеть со своего места.

На носилках лежал человек в милицейской форме. На погонах — это было видно четко — было три больших звезды и два просвета. Пришлось напрячься, чтобы хотя бы понять, что звание достаточно высокое: еще чуть-чуть, и начинаются генералы. Никаких внешних повреждений на теле видно не было, форма немного испачкана грязью, словно его волокли по земле. Следов крови нигде не обнаруживалось...

«Странно, чего это с ним случилось? Судя по эскорту, тут явно не инфаркт. Ладно, чего гадать? Еще три минуты, и залезу внутрь, все узнаю...»

— Галина, возьмите себе в помощники вот, товарища (он махнул рукой в того, кто пытался объяснить генералу сущность Франкенштейна) и разденьте труп на носилках... Галина, я понимаю, помню, что собирался вас отпустить. Вы только помогите раздеть, и можете быть свободны.

Лаборантка оставила все свои дела и направилась к носилкам. Офицер тоже подошел следом за ней. Они расстегнули китель, сняли галстук...

— Думаю, до пояса будет достаточно, — внезапно произнес генерал, когда Галя принялась расстегивать ремень на брюках трупа.

— Я так не думаю, — вмешался Венечка, к этому времени закончивший свою работу. — Мне он нужен полностью...

— Слушайте меня... — отшвырнул генерал окурки на пол. — Мне нужно знать... Что... У него... В голове! И все!

Смирнов вздрогнул.

— В... В голове? А что там?... Что в голове может быть такого? Вы бы хоть объяснили мне, что случилось?

Генерал подошел к нему вплотную — так близко, что врач ощутил его прокуренное дыхание.

— Меньше знаешь — лучше спишь. Вскроешь черепную коробку, напишешь нам бумагу о неразглашении и забудешь, что мы здесь были!

Смирнов понял, что генерал говорит так, чтобы Галина его не слышала.

— Бабу свою гони отсюда быстрее! И не дай бог она проболтается...

Венечка коротко кивнул, повернулся к носилкам, где в ожидании застыла лаборантка:

— Галочка, вы свободны... Завтра без опозданий...

Он развел руками в стороны, словно объясняя, что не виноват, но такие вот обстоятельства... Лаборантка понимающе кивнула и выскочила в раздевалку. Через минуту цокот каблучков сообщил о том, что она умчалась домой.

— Приступайте! — приказал генерал. — И, чем быстрее, тем лучше для всех нас!

Венечка подошел к носилкам, присел на корточки рядом с полуобнаженным трупом и прикоснулся к правому запястью. Он так делал всегда перед вскрытием каждого, кого приносили к нему в более или менее целом виде. Он уже не помнит, почему это стало своего рода ритуалом, но без этого работа уже не обходилась. Венечка словно просил прощения у того, кто лежал пе-

« Приходит мужик на работу, а там — гора трупов!.. »

ред ним, за то, что будет твориться ближайший час.

Кожа оказалась еще не совсем холодной.

— Когда он умер?

Генерал взглянул на часы и ответил:

— Пятьдесят минут назад.

Венечка кивнул, поднялся и попросил помочь поднять тело на стол. И случилось невероятное: сам генерал шагнул к нему, подsunул руки под плечи трупа и поднял глаза на своего помощника в ожидании:

— Ну, чего ждем? Давай по-быстрому!

Втроем они закинули тело на стол, как пушинку. Похоже, генералу сил было не занимать. Форменные ботинки на ногах умершего глухо стукнулись друг о друга. Генерал отряхнул ладони и отошел на пару шагов в сторону.

— Если надо помочь, доктор. Не сомневайся, поможем, — сказал он, оглянувшись в поисках стула и присел возле стеклянного шкафа с инструментами. Венечка кивнул, зашел со стороны головы, подsunул под плечи деревянную подставку с выемкой для шеи и приподнял веки мертвеца, желая заглянуть тому в глаза...

От внезапного вскрика врача генерал резко выпрямился и подбежал к столу. Смирнов вдруг осознал, что за истекшие мгновения оказался на пару метров от трупа. Пальцы мелко и предательски тряслись.

— Что там такое? — генерал встал между мертвецом и врачом. — Что вы видели?

Венечка трясающейся рукой молча указал на лицо. Генерал посмотрел туда, куда ему указали, и указательными пальцами отодвинул веки трупа, как и доктор несколько секунд назад.

Глаз... не было. Вместо них неровные шары с перемешанной внутри разноцветной массой. Никакого подобия зрачков, радужки, — ничего! Какие-то жуткие глобусы Юпитера...

— Твою мать... — процедил сквозь зубы генерал. — Вот как оно, значит, бывает...

И он внезапно замолчал, поняв, что брякнул лишнее.

— Что бывает? — зацепился за последние слова Венечка. — Что все это значит?! Я не могу работать, не понимая, что делаю!

Голос сорвался чуть ли не на визг.

— Вам придется делать свою работу, — генерал полез в карман за еще одной сигаретой. — Судьба, знаете ли. Так получилось, что выбор пал на вас. Случайный выбор, поверьте. А сейчас хватит криков. За работу, уважаемый. Как ваше имя?

— Вениамин, — уже тише сказал Смирнов.

— Очень приятно. Афанасий Сергеевич Ливанов, генерал-майор милиции. Для начала хватит...

Ливанов кивнул в сторону инструментов.

— Помогать?

Венечка замотал головой.

— Но в начале же надо все задокументировать... Протокол и все такое. Сфотографировать, измерить, описать. Есть руководящие документы, которые все это регламентируют.

— Понимаю, Вениамин. Но все это — не сейчас. Да и вообще вряд ли понадобится. Ты, главное, голову вскрой. Мы его потом унесем, никто и не узнает. Считай, так, халтурка... А ведь у патологоанатомов такое вряд ли встречается. Насчет вознаграждения не заморачивайся: деньги, если хочешь, вперед.

Он полез в карман и вытащил толстый бумажник.

Смирнов смотрел и слушал, будто загипнотизированный. Он вообще плохо понимал, что здесь происходит. Машинально поправив свет над столом, он взял из рук генерала несколько купюр, отметив про себя, что это доллары, после чего взял из шкафа необходимые инструменты и встал у изголовья.

Снятие скальпа — дело не самое трудное, особенно если скальпель отменно наточен, а за плечами сотни подобных вскрытий. Кожа

вместе с волосами была снята с затылка спереди и закрыла собой ужасные глаза, обнажив окровавленные кости черепа. Вениамин прошелся по ним пальцами, определил отсутствие линий переломов, пощуповал руками, как вращается шея, и убедился, что позвонки целы.

Генерал наблюдал за ним с нескрываемым интересом. Он курил уже неизвестно какую по счету сигарету, наполнив дымом прозекторскую. Вот Смирнов взял пилу, пристроил ее ко лбу мертвеца...

Звук был неприятным. Ливанов вдруг понял, что ему хочется выйти отсюда на воздух. И не потому что вдруг стало плохо. Этот звук... Чертовое жужжание пилы... Он с трудом подавил желание сбежать и заставил себя смотреть.

Скоро появились красные опилки, это говорило о том, что зубья пилы раздирают сосудистую оболочку мозга. Смирнов в нескольких местах ударил долотом, снова подправил распил ножовкой...

И вдруг на стол из черепной коробки вылилась жидкость, желто-розовая, словно лимонад. Вениамин отступил на шаг, глядя, как крупные капли стекают на пол, и понял, что столько жидкости в норме внутри быть просто не может. Он аккуратно подцепил отпиленный свод и не успел подхватить его: кость упала на пол с отвратительным грохотом.

Смирнов удивленно и одновременно с ужасом смотрел внутрь оторванного черепа. Генерал подошел и тоже заглянул туда, где полагалось быть мозгу.

ВНУТРИ НИЧЕГО НЕ БЫЛО.

Череп был пуст. Лишь кое-где в естественных ложбинах осталась та самая желто-розовая жидкость, которая залила стол и пол. Основание черепа было гладким и ровным, без признаков повреждений.

— Что это значит? — наконец оторвался от созерцания пустоты Смирнов. — Кого вы мне привезли?

Он вплотную приблизился к Ливанову и понял, что ответа не дожидается, судя по всему. Тот ожидал чего угодно, но только не то, что увидел.

Через несколько секунд генерал сумел выдавить из себя что-то, похожее на кашель. Больше никаких звуков от себя он не добился. Смирнов провел пальцем по внутренней поверхности черепных ямок, убеждаясь в том, что все это не сон.

— Советую рассказать мне хотя бы часть правды, если, конечно, больше вам от меня ничего, кроме этой работы, не надо, — процедил сквозь зубы Венечка. — Или вы сейчас уходите, и я забываю о вас, как о страшном сне, или придется делиться...

— Не думаю, что в этом есть смысл, — внезапно вышел из ступора генерал. — Хотя... Вы бы могли здесь провести анализ той жидкости из черепа? У вас для этого хватит ума, времени, аппаратуры?

— Зачем? — спросил Венечка. — В этом есть какой-то глубинный смысл? Что надо было сделать с человеком, чтобы его мозги превратились в лимонад? И не говорите мне, что его мама родила так, что у него мозгов не оказалось, как у всех ваших работников.

— Смысл есть всегда, — Ливанов отошел в сторону, вынул из кармана сотовый телефон и набрал чей-то номер.

— Да, это я... — тихо говорил он, особо не таясь от ушей Смирнова. — Буткевич мертв. В голове пусто... Не у меня — у него. Не надо мне хамить, сами понимаете, вина целиком ваша. Да, мозги превратились в воду... Мощнось? Я думаю, он сам решил, какую мощнось выставить на генераторе...

Ливанов отодвинул телефон от уха, демонстративно не обращая внимания на бульканье тирады в ответ. Смирнову не удалось разобрать ни слова, но, похоже, на генерала вылилось гнева сверх всяких пределов.

— Не думаю, что... Что?! Через... У меня мало времени, чтобы принять решение. Это очень маленький срок. Я не... Черт!

Он выключил телефон и посмотрел на Смирнова, словно собираясь сказать ему нечто сверхъестественное.

— Что?.. Что случилось? — Венечка даже стал ниже ростом.

— Везут. Еще шестерых. Я думаю, что все будет то же самое: вода вместо мозгов.

Ливанов опустился на стул и прислонился к шкафу. Инструменты в шкафу сиротливобрякнули внутри. Пустые баночки из-под майонеза, предназначенные для макропрепаратов, издали загадочную тоскливую мелодию.

Все стихло.

И тогда Смирнов вспомнил о Тушине...

Машину он оставил у самых дверей. Быстрый взгляд на милицейскую «Волгу», на пару «УАЗиков», какие-то причудливые подозрения... Несколько человек курили в сторонке, о чем-то перешептываясь и сплевывая себе под ноги. Огоньки сигарет ярко вспыхивали в темноте возле морга, освещая напряженные измученные лица.

— Как-то многовато их... — подумал Тушин, открывая скрипучую дверь. — Лучше бы на дорогах стояли, всяких дальнотойщиков к порядку призывали, глядишь, и поспокойнее бы... Было на дорогах, — размышлял он, войдя внутрь и столкнувшись нос к носу со Смирновым. Тот нервно шагнул поперек коридора, глядя куда-то в пустоту, и теребил ставший уже навсегда серым халат. Фартук валялся неподалеку на полу, показывая на себе множество разводов бурого цвета.

— Что случилось? — спросил Тушин. — Только коротко, — он сделал предостерегающий жест рукой, поняв, что Венечка сейчас пустится в пространные объяснения. Смирнов, наткнувшись на этот взмах ладони, проглотил рвущиеся наружу слова, выдохнул, закрыл глаза, досчитал про себя до десяти и сказал:

— Семь трупов.

— Неплохо для ночи, — изрек Тушин, направляясь к себе в кабинет. — Не останавливайся, докладывай на ходу.

— Все семеро — высокие милицейские чины, — семенил сзади Петра Михайловича Венечка, — Аж генерал приехал на них посмотреть, кстати, фамилия Ливанов, генерал-майор, чего-то очень сильно скрывает. И кто-то на него ох как орет по сотовому...

Тушин внезапно остановился, Венечка ткнулся ему в спину.

— Ты меня вызвал потому что тебе в тягость семь вскрытий сделать за ночь?

— Вы что, Петр Михайлович! — едва не задохнулся Смирнов. — Как вы могли так подумать? Я ленью никогда не отличался... Просто там такое... Такое!

— Что там может быть? — недоверчиво спросил Тушин, войдя в кабинет и натягивая на пиджак халат. Потом понял, что что-то не так, снял пиджак, за ним галстук и вдруг понял, что даже среди ночи оделся как на прием к мэру.

— У них что-то с мозгами, — развел руками Смирнов. — И я думаю, только Ливанов знает, что случилось. Я вскрыл одного по приказу генерала. Только череп. Там пусто. Только полтора литра какой-то таинственной жидкости розового цвета...

— Нормальный милицейский череп, — брякнул, не вслушиваясь в слова Смирнова, Тушин. — Пусто... То есть как «пусто»?!

— Вот то-то и оно, — развел руками Венечка. — А вы — «лень, лень»... Суть-то в том, что у остальных шестерых, которых привезли через тридцать минут после первого, симптомы те же. Полное отсутствие глазных яблок в том понимании, в каком мы можем их представить себе. Какие-то водянистые шары... Как желток с белком перемешано все, вот только цвет коричневый. Ну, а раз с глазами такая фигня, то я даже вскрывать без вас не стал. Сказал генералу. Он подумал и согласился, чтобы я вам позвонил. Вот так вы здесь и оказались.

Тушин застыл, сумев засунуть только левую руку в помятый рукав. Правая сделала какой-то неопределенный жест в воздухе нечто вроде «Ага... Страшная сказка на ночь»... Смирнов смотрел на собеседника не в силах понять, что творится внутри у заведующего: поверил, не поверил, что скажет, какими словами выматерит?

— Короче, кадаверы качественные, — внезапно раскрыл рот Тушин и закончил одеваться. Халат после громкого хлопка вытянулся на спине. Петр

Михайлович сунул руки в карманы, взглянул прямо в лицо своему сотруднику и, казалось, даже прислушался к дыханию: не пил ли тот? — Ну-с, идем.

И они отправились в секционный зал.

Войдя в помещение, освещенное несколькими яркими операционными лампами, Тушин немного прищурился и тут же отыскал глазами генерала. Ливанов медленно переходил от стола к столу, вглядываясь в лица трупов. Столов было всего четыре. Трое остальных, которым не нашлось места, остались на носилках около стены с дверями, ведущими в холодильники. Кто-то аккуратно сложил им на груди фуражки. Неподалеку на столике для инструментов, на серо-коричневой простыне, лежали три кобуры с пистолетами и четыре укороченных «Калаша».

Генерал увидел, что в помещение вошел кто-то еще в белом халате. Тушин коротко кивнул, явив свои аристократические штучки даже здесь, в морге.

— Показывай, — подтолкнул он Венечку. Они подошли к вскрытому черепу. Петр Михайлович машинально протянул руку, но вдруг понял, что ходит без перчаток, и на полпути остановился. А через секунду любопытство пересилило.

Он провел пальцем по костям черепных ямок, ощутил каждую выемку, каждое отверстие, каждый бугорок... Этого просто не могло быть. Человек, который еще час назад в милицейской форме шел по улице, имея на поясе пистолет Макарова, а в кармане удостоверение, внезапно лишился мозга! И не просто лишился. То, что было мозгом, стало какой-то цветной жидкостью; Тушин приблизил к глазам мокрый палец, внимательно рассмотрел его, потом понюхал...

Смирнов был готов поспорить на все, что угодно, что Тушин сейчас лизнет каплю, готовую упасть на пол. К счастью, этого все-таки не случилось. Доктор вытер палец о полу халата и поднял взгляд на Смирнова. Тот молча пожал плечами и отодвинулся в сторону, потому что услышал, как сзади к ним подходит генерал.

— Что вы на это скажете? — спросил Ливанов. Спросил так, как будто они продолжили начатый давно разговор, как будто не надо было представляться, что-то объяснять, о чем-то просить.

— Пока ничего, — коротко ответил Тушин. — Поживем увидим. Вениамин, возьмем, ну... Хотя бы вот этого.

И они отошли к следующему столу. Венечка сбегал за ножовкой и скальпелем, открыл потихоньку кран с водой у изножья. Они вдвоем запрокинули тело на деревянный чурбак, свесив через него голову трупа. Смирнов взял в руки шланг и направил вялую струйку воды себе под ноги, на канализационную решетку стока.

Тушин решительными движениями принялся выполнять ту же работу, что и Венечка около часа назад. Сразу же среди сопровождающих нашлись желающие выйти подышать свежим ночным воздухом. Зал опустел (если можно назвать пустым зал, в котором, кроме двух врачей и генерала милиции, находились семь трупов). Привычно жужжала ножовка, привычно стучало долото... И под ноги докторам вылилась желто-розовая жидкость.

Смирнов успел подставить банку. Набралось примерно стакан, остальное пришлось смыть в канализацию струей воды. Ливанов смотрел на все происходящее отсутствующим взглядом, постукивая пальцами по кобуре. Тушин видел перед собой пустой череп и не понимал, проснулся он полтора часа назад или все это ему снится...

— Все то же самое, — произнес Ливанов, ни к кому не обращаясь. — Думаете, стоит продолжать? — и он махнул рукой на остальных.

Петр Михайлович отошел от стола, присел у окна, покрашенного до половины белой краской, и попытался разглядеть в маленькое отверстие, выкопанное чьим-то ногтем много лет назад, что творится на улице. Покачивающийся фонарь выхватывал из мрака какие-то непонятные очертания, тени то удлинялись, то исчезали совсем...

— Что вы от меня хотите? — спросил он генерала после пары минут раздумий. — Чтобы я объяснил вам, что это такое? Мне кажется, это под силу сделать вам, но никак не мне. Ведь все эти тела здесь — неспроста их сопровождает человек с большими погонами, неспроста... Ведь столько человек никогда сразу не умирает, если только не случается что-то из ряда вон. А тем

более сразу семь сотрудников вашего ведомства.

Ливанов наклонил голову, слушая все это, потом подошел и встал рядом, прислонившись к стене.

— Вы правы, — он взглянул вверх белой краски, в сторону деревьев. — Но у меня нет другого выхода. Я вел этих людей... Я отвечаю за них. И еще отвечу. Я сам понимаю, что продолжать нет смысла. В остальных пяти головах, скорее всего, то же самое.

И тут всех удивил Венечка.

Он отступил на шаг, прикусил губу. И произнес:

— Петр Михайлович... Это синяя птица...

— Что? — не поняв, о чем речь, спросил генерал.

— Это бывает раз в тысячу лет... Чтобы такая удача... — Венечка развел руки в стороны, пытаясь обнять воздух. — Ведь такого никогда еще не было! Никто не знал, что такое может быть!

— Удача?! — поднял брови Ливанов — Смерть семерых подчиненных — удача?! Что вы несете?

— Да это же Нобелевская премия. Как вы не понимаете?! — закричал Венечка в пустоте зала. — Мы в одном шаге от грандиозного открытия! С этими людьми случилось что-то из ряда вон выходящее, мы просто обязаны описать это, явить это миру и получить всю причитающуюся нам славу первооткрывателей!

Тушин выслушал эту тираду и опустил глаза в пол. Он был уверен, что все не так просто и радужно...

Генерал сжал кулаки, пальцы хрустнули. Смирнов вздрогнул от этого звука и посмотрел в глаза Ливанова. Тот с трудом сдерживал себя.

— Во-первых, это государственная тайна... — начал генерал, но тут же понял, что говорить надо не об этом. — Да причем здесь... Я могу вам все объяснить. Если хотите. Правда, вы станете невольными соучастниками. Но я ни за что не хотел бы, чтобы из этой истории получилась Нобелевская премия. Она по определению недостойна...

Он хотел было продолжить, но Тушин внезапно остановил его жестом и спросил:

— Чем нам будет грозить это знание? Парой подписей в бумагах? Смертью? Чем? Только честно. Вполне возможно, я не захочу слушать.

Ливанов замер на полуслове. Казалось, он не ожидал подобного вопроса. Оттолкнувшись от стены, генерал прошел вдоль столов к тем трупам, которые лежали на носилках, прикоснулся к пистолетам на столе. Было видно, что ему нужно время, чтобы собраться с мыслями. Пауза затягивалась. Нетерпеливый Смирнов перевел взгляд со своего заведующего на генерала и ждал. Ждал и Тушин.

— Кто-нибудь из вас испытал сегодня что-нибудь необычное? — спросил Ливанов оттуда, от стола с оружием. — Ну, какие-нибудь видения, неприятные ощущения, черт его знает, что еще! Я не могу описать весь спектр тех явлений, которые могли посетить вас! Я просто не в состоянии, потому что не имею об этом полного представления!

Тушин поднялся и, склонив голову, с силой зажмурил глаза.

Дальнобойщик на краю дороги.

Визг тормозов, листья, которые ветер швырял ему на лобовое стекло.

Падающее дерево.

Запах горелой резины.

— Было, — ответил он. — Было. Вы можете это объяснить?

— Могу. Хотите ли вы это услышать?

— Теперь да, — кивнул Тушин. — Одно из таких видений случайно или не случайно спасло мне жизнь по дороге сюда. Говорите.

Венечка опустился на тот стул, который освободил Петр Михайлович, и прислонился затылком к холодному кафелю.

— Сегодня на одном из секретных полигонов Министерства внутренних дел проводилось испытание нового оружия... Не совсем нового, аналоги существуют уже некоторое время, но по силе сегодняшней экзemplя превосходил все, что было раньше, в разы. По определению у милиции не может быть какого-то сверхмощного оружия, и это действительно так, тут уж поверьте: тот по-

лигон находится совсем рядом с кольцевой. Практически среди людей...

Ливанов остановился, собираясь с мыслями. Первые предложения дались ему явно с большим трудом, он находился под мощным давлением чувства долга и государственной тайны — двух составляющих всей его службы.

— Вы где живете, доктор? — обратился он к Тушину. — Не отвечайте, для меня главное район. Где-то на севере Москвы?

Петр Михайлович кивнул.

— Значит, я угадал, — Ливанов криво улыбнулся. — И вас зацепило...

Тушин хотел спросить, чем зацепило и почему, но вдруг понял, что Ливанов сам все расскажет. По порядку. И Ливанов продолжил:

— Это оружие из того разряда, которое называют психологическим. Уже давно над нашим и не только над нашим ведомством витает мысль: «Как бы научиться воздействовать на умы толпы, чтобы не дать ей совершать всякие противоправные действия?» Извините, ничего не поделаешь, язык казенный, привык. Так вот, разные излучатели, устройства для подавления воли пытались изобрести давно. Проверяли их разными способами: на животных, на заключенных... Вроде бы работало, но эффект был уж очень непостоянным. То, что заставляло одних убежать в страхе, у других вызывало лишь улыбку.

— Разброс был огромным, — вставил слово Тушин. — Но ведь это логично: человеческий мозг настолько непредсказуем, что просчитать все варианты воздействия на ментальную сферу невозможно.

— Вы правы, но лишь частично, — ответил Ливанов. — Да, разброс ответов велик. Но варианты конечны. Теперь мы это знаем.

— То есть оружие создано? — внезапно спросил Венечка. — И вот это... — и он ткнул пальцем в носилки перед генералом. Тушин вздрогнул — он еще не зашел в свои рассуждения так далеко.

— Это не совсем то, о чем вы думаете, — железным голосом произнес Ливанов. — Но это результат действия изобретенного оружия. Действия не по назначению.

— То есть? — Петр Михайлович подошел вплотную к генералу и остановился рядом, тоже положив пальцы на оружие. Так ему было немного спокойнее, хотя он чувствовал, что предательская дрожь скоро распространится на все тело.

— То есть... Секретная информация, — отступил на шаг Ливанов. — Я не могу объяснить, из-за чего, но скажу, что они покончили с собой. Все. Это самоубийство.

— Коллективное самоубийство? Из этого вашего секретного оружия? — Тушин смотрел на генерала широко раскрытыми глазами. — Но почему?!

Ливанов снова сделал шаг назад. Чувствовалось, что близость доктора выводит его из равновесия, он стал шумно дышать и покраснел.

— Понимаете, у них был выбор... Не могу, секретная информация!!! — закричал он, схватил со стола автомат и направил его на Тушина. — Что ты тянешь из меня клещами? Прокурор? Не твое дело!!! Отойди!

Петр Михайлович отступил немного назад и с грустью взглянул на Ливанова. Он несколько не боялся оружия: он был уверен, что генерал не выстрелит. Тушин понимал, что еще несколько минут разговора в подобных тонах, и генерала хватит инфаркт.

— Отошел, отошел... — тихо сказал доктор. — Опустите автомат. Лучше расскажите — облегчите душу.

Ливанов отвел ствол в сторону, но не опустил «Калашников».

— У них был выбор, понимаете?! Применить это оружие против людей или против себя, — Ливанов говорил быстро, Тушин едва понимал слова. — Завтра в Москве будет... Черт его знает, что будет завтра твориться в Москве, а все мои лучшие люди мертвы! Они не поняли простой мысли: что если не они будут использовать это оружие, на их место найдут других, не понимающих всего кошмара происходящего!

« В остальных
пяти головах,
скорее всего, то же
самое »

— Они применили его против себя, — закончил монолог генерала Тушин.
— Да, — кивнул Ливанов. — Они включили генератор на полную мощность, встали вокруг и один из них — я даже могу догадаться, кто, я служил с ними много лет... И один из них произвел воздействие. Проще говоря, нажал кнопку.

— Какое сегодня число? — внезапно спросил Тушин.

— Второе... Нет, уже третье октября, — машинально сказал Ливанов.

— Ладно, неважно... По-моему, все было не так. Сначала один из них попробовал его на себе и погиб, — пристально глядя на Ливанова, проговорил Петр Михайлович. — А потом оставшиеся в живых решили, что уйти надо всем. И вот тогда, когда я ехал сюда, они тоже покончили с собой. И этой волной зацепило и меня... Когда я ехал сюда, у меня были кратковременные галлюцинации, они спасли мне жизнь. Нечто вроде дара предвидения. И теперь, генерал, никто не знает, во что превратились мои мозги.

Ливанов с трудом откашлялся, выслушав все, что сказал ему сейчас Тушин.

— Что это за оружие? Поподробнее, пожалуйста, — Петр Михайлович мягко, но настойчиво потребовал от генерала правды.

— Генератор эмоционального фона, — Ливанов совсем опустил руки, ствол автомата был направлен в пол. Смирнов до этого не отрывал глаз от оружия, а теперь немного успокоился и полностью сосредоточился на том, что говорил генерал. — Такая штука, которая может (теперь я точно в этом уверен) заставить людей совершать запланированные поступки.

— Какие? Что будет завтра в Москве? — спросил Смирнов.

— Уже не завтра — сегодня, — ответил ему, не поворачивая головы, Ливанов. — Будет война. Маленькая война. Политика, с этим ничего не поделаешь. Я один из посвященных. Я отвечал... И пока еще отвечаю за ментальную составляющую. Мое спецподразделение будет воздействовать на людей с помощью генератора.

— Какая к черту война?! На дворе двадцатый век, Москва, о чем вы говорите?! — Тушин вплотную приблизился к Ливанову, но тот уже и не делал попыток отступить.

— Я же говорю — политика... Еще полвека спустя никто даже не разберет, кому и что было надо. Сидите завтра дома, и все обойдется.

— Уже ничего не обойдется, уже есть жертвы, разве вы не понимаете?! — Тушин не находил себе места.

— Это не жертвы, — изменившимся, каким-то чужим голосом произнес Ливанов. — Это ничтожная толика... Никто и не заметит... Завтра у Дома правительства будет бойня. Я давал присягу. Я не смогу уйти так, как они... У меня не хватает сил. Отойдите, — и он повел стволом в сторону Тушина.

— Петр Михайлович, лучше отойдите от этого сумасшедшего! — крикнул со своего места Смирнов.

— Вот-вот! Петр Михайлович, он дело говорит, — Ливанов усмехнулся. — Отойдите, а я буду замечать следы.

Едва Тушин отошел в сторону, генерал поднял автомат и выпустил очередь в носилки у дверей. Грохот автоматной очереди заставил людей с улицы вбежать внутрь. Ливанов остановил их жестом, отрицательно покачал головой, потом продолжил. Пули рвали форму на милиционерах, гнули и вколачивали в тела значки и ремни; Тушин заметил, что генерал старается попасть им в головы. Через минуту магазин закончился. Стало тихо.

В ушах тихонько звенело. Петр Михайлович подошел к носилкам, посмотрел. Понять, от чего погибли эти люди, патологоанатому было бы нетрудно. Ни одна рана не кровоточила — любой студент-медик догадается, что они нанесены после смерти.

— Врач поймет, — угадал мысли Ливанов. — В крематории разбираться не будут. А эти, — он кивнул на трупы на столах, — их я заберу в мешках. Эй, вы где там? — он позвал остальных. — Выносим. Кто-нибудь догадался вызвать грузовик? Пока трупы выносили, оставляя на полу брезентовые лох-

мотья от простреленных носилок, Ливанов отошел в сторону и позвонил кому-то по сотовому.

— Я думаю, имеет смысл расстреливать трупы, которые сегодня будут на площади... — говорил он в телефон. — Кто там будет разбираться, от чего они умерли... Да, если что-то пойдет не так, мы поднимем мощность до критической... Готовьте крематории, ставьте там своих людей, которые не будут задавать вопросы... Я готов. Приказывайте.

И они все ушли. Во дворе рыкнул грузовик, увозя в кузове в пекло крематория тайну существования страшного оружия.

Тушин заложил руки за спину и принялся расхаживать вдоль столов, пиная звонко бряцающие на кафеле гильзы.

— Надо бы прибраться, — сказал он. — А то завтра никому не объясним, что здесь было.

— А на полу? Там, где носилки стояли? Там же кафель расстрелян, — Смирнов подошел поближе, носком ботинка пошевелил осколки.

— Завтра... Я думаю, что здесь завтра будет много работы, — Петр Михайлович повернулся к Венечке. — Ночной работы. Что там сказал Ливанов? «Сидите завтра дома, и все обойдется»... Ты едешь? Я подброшу, если хочешь.

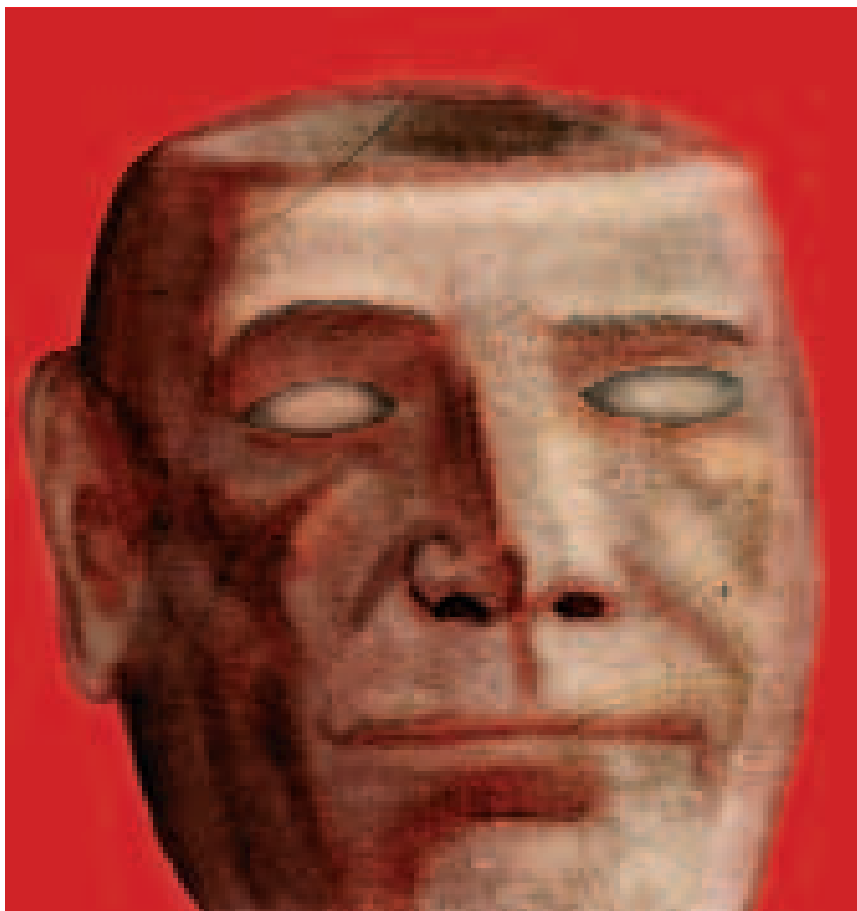
Смирнов кивнул, продолжая смотреть себе под ноги. Потом он наклонился, поднял одну гильзу и сунул в карман халата.

— На память, — сказал он сам себе. — О третьем октября одна тысяча девятьсот девяносто третьего года. Вы будете сидеть дома?

— Не знаю, — сухо ответил Тушин. — Вряд ли. Ливанов же обещал. Ночная работа...

Они переоделись, сели в машину Тушина и уехали в ночь.

А где-то уже грохотали танки...



Lifé's Good



FLATRON™
freedom of mind



FLATRON F700P

Абсолютно плоский экран

Размер точки 0,24 мм

Частота развертки 95 кГц

Экранное разрешение 1600x1200

USB-интерфейс



Dina Victoria
(095) 688-61-17, 688-27-65
WWW.DVCOMP.RU

Москва: АБ-групп (095) 745-5175; Акситек (095) 784-7224; Банкос (095) 128-9022; ДЕЛ (095) 250-5536; Дилайн (095) 969-2222; Инкотрейд (095) 176-2873; ИНЭЛ (095) 742-6436; Карин (095) 956-1158; Компьютерный салон SMS (095) 956-1225; Компания КИТ (095) 777-6655; Никс (095) 974-3333; ОЛДИ (095) 105-0700; Регард (095) 912-4224; Сетевая Лаборатория (095) 784-6490; СКИД (095) 232-3324; Тринити Электроникс (095) 737-8046; Формоза (095) 234-2164; Ф-Центр (095) 472-6104; ЭЛСТ (095) 728-4060; Flake (095) 236-992; Force Computers (095) 775-6655; ISM (095) 718-4020; Meijin (095) 727-1222; NT Computer (095) 970-1930; R-Style Trading (095) 514-1414; USN Computers (095) 755-8202; ULTRA Computers (095) 729-5255; ЭЛЕКТОН (095) 956-3819; ПортКом (095) 777-0210; **Архангельск:** Северная Корона (8182) 653-525; **Волгоград:** Техком (8612) 699-850; **Воронеж:** Рет (0732) 779-339; РИАН (0732) 512-412; Сани (0732) 54-00-00; **Иркутск:** Билайн (3952) 240-024; Комтек (3952) 258-338; **Краснодар:** Игрек (8612) 699-850; **Лабитнанги:** КЦ ЯМАЛ (34992) 51777; **Липецк:** Регард-тур (0742) 485-285; **Новосибирск:** Квеста (38322) 332-407; **Нижний Новгород:** Бюро-К (8312) 422-367; **Пермь:** Гаском (8612) 699-850; **Ростов-на-Дону:** Зенит-Компьютер (8632) 950-300; **Тюмень:** ИНЭКС-Техника (3452) 390-036.

Поручите бумажную работу профессионалам.



Где бы Вы ни работали, в маленькой фирме или в огромной корпорации, Вы сможете подобрать принтер Samsung, отвечающий потребностям Вашего офиса. Служба поддержки пользователей Samsung обеспечит бесперебойную работу Вашей техники.

Доктор Принтер

Диагностировать
принтер



**Техническая поддержка
пользователей:**

<http://e-support.samsung.ru>

Сайт для партнеров:

<http://partners.samsung.ru>

**Консультации для корпоративных
клиентов:**

(095) 540-42-19, 540-42-33, 540-42-38



ML-2250/2251N/2251NP/2252W

- Скорость печати: 20 стр/мин
- Разрешение: 1200x1200 dpi
- Языки управления печатью: PCL6, IBM ProPrinter, EPSON, PostScript3 (2251NP)
- USB и параллельный порт
- Ethernet 10/100 Base TX+802.11b (2251N, 2252W)
- Память: 16-144 Мбайт



ML-2550/2551N/2552W

- Скорость печати: 24 стр/мин
- Разрешение: 1200x1200 dpi
- Языки управления печатью: PCL6, IBM ProPrinter, EPSON, PostScript3
- USB и параллельный порт
- Ethernet 10/100 Base TX+802.11b (2551N, 2552W)
- Память: 32-160 Мбайт



ML-3560/3561N/3561ND

- Скорость печати: 33 стр/мин
- Разрешение: 1200x1200 dpi
- Языки управления печатью: PCL6, IBM ProPrinter, EPSON, PostScript3
- USB и параллельный порт
- Ethernet 10/100 Base TX (3561N, 3561ND)
- Память: 32-288 Мбайт

SAMSUNG



электронные деньги

12.05(61)