

# Прощай, мышъх!

Николай Лихачев, которого весь айтишный (и не только) мир знает как Криса Касперски, а также мышъха, ушел из жизни. Ушел безвременно, оставив после себя более 20 книг, множество завершенных и незавершенных ИТ-проектов и признанный авторитет лучшего хакера Земли

«Системный администратор» был первым изданием в России, где Крис из номера в номер печатал свои статьи, сложившиеся позже в книги. И одним из немногих СМИ, которому Касперски, несмотря на свою закрытость и нелюбовь к прессе, никогда не отказывал в интервью – ни в «русский», ни в «американский» период жизни и работы.

Отдавая дань уважения памяти российского обладателя американской визы 01 (для людей с выдающимися способностями, которую дают, к примеру, нобелевским лауреатам), мы публикуем в сокращении некоторые наши архивные материалы.



## Романтичный хакер Крис Касперски

«Системный администратор» № 12, 2006 год  
<http://samag.ru/archive/article/1679>

### Самородок

Вундеркинд? Сам Касперски так не считает:

– Я смотрю, у многих моих знакомых дети в шесть лет «прогу» уже умеют компилировать. Прогресс... Я же начал тогда, когда появились доступные компьютеры.

Мой первый компьютер – «Правец 8D» – был совершенно несовместим ни с «синклерами», ни с «бэкашками», имевшими хождение в народе, и кучей программного обеспечения. У меня же не было ничего, кроме платы с несколькими микросхемами, и, чтобы вдохнуть в них жизнь, требовалось научиться программировать, это затянуло неожиданно.

Однако после школы Крис пошел учиться на радиофизика. Высшее образование – яркая страница его биографии. Успешно поступив в Таганрогский радиотехнический институт, и, проучившись там три месяца, Крис понял, что он и вуз – вещи несовместимые:

– Я человек неорганизованный, а там много обязательности. А просто так зубрить, чтобы сдавать, мне не хотелось. Ушел, но на следующий год родители уговорили снова поступать – мол, нельзя ведь без образования остаться. Поступил еще раз, но история повторилась. И в третий раз поступил и опять не выдержал.



## Автор

– Последние месяца три у меня такой темп – один день на статью. За один день успеваю статью написать, отредактировать, подготовить картинки. Компоную материал для следующей статьи, после чего падаю замертво на клавиатуру. Утром просыпаюсь и начинаю быстро строчить вторую статью. А еще впереди третья, четвертая, пятая, до бесконечности... А вообще я на статью трачу дня два. Но если серьезная тема, бывает, неделя требуется.

### – А что вам нужно, чтобы написать хорошую статью? Вдохновение?

– Не столько вдохновение, сколько материал. Допустим, для «Системного администратора» я писал много статей по файловым системам: NTFS, ext2/3fs, USF. Сначала их исследовал, а потом обобщал в виде статьи. Обычно статье предшествует исследование. Мне нравится писать о том, в чем я разбираюсь, тут я могу принести людям пользу. Любимые темы – дисассемблирование, отладка, защита, взлом. Это мое. Я этим занимаюсь и могу эту тему развить, потому что сам не раз это делал. Имею опыт.

### – Самая интересная для вас тема – безопасность?

– Хакерство. Мне интересно заглянуть «под капот» программы, защиты. Тут нетривиальное мышление требуется.

### – Вас привлекает тайна?

– Возможность пойти нехоженым путем. Интересно. Сммотришь систему защиты даже не ради того, чтобы взломать и бесплатно пользоваться программой, а чтобы себя проверить, выиграть в состязании с машиной. Она меня перехитрит или я ее?

### – Вы начали работать на компьютерах, потому что было интересно. А как менялось отношение к информационным технологиям в течение жизни?

– Раньше компьютеры менялись медленно. Я знал о них все. А сейчас – слишком быстро. Мне неинтересно читать о новых железяках. Если ими торгуют, то продавец сам

расскажет, если не торгуют, то зачем об этом читать? Раньше процессор расковырял, что-то о нем узнал – и эти знания можно долго использовать, потому что парк компьютеров не обновлялся годами. А теперь все быстро меняется, и смысл детальных раскопок теряется.

### – Как вы считаете, какие качества нужны человеку, который решил посвятить жизнь ИТ?

– Во-первых, программист – это инженер, а инженерная профессия – это учет рисков, умение просчитывать, при каких условиях конструкция откажет, когда надо делать дополнительные подпорки, а когда нет. Поэтому хороших программистов не очень много. Нужно иметь инженерное мышление и математическое отчасти. Плюс нужна усидчивость. Приходится читать много документации, на английском языке, постоянно работать над собой. Не бывает так: человек выучился в университете, поступил на работу и может программировать. С другой стороны, все программисты в значительной степени обладают качествами аутистов, т.е. людей, которые стараются не контактировать с окружающими, им интересен только их внутренний мир и дело, которому они посвятили жизнь.

## Одиночка

Он честно признается в своих «нелюдимах» качествах, принимает свою природу как данность и бороться с ней не пытается. «Хотя я написал кучу книг, взломал кучу программ, а защитил еще больше, но фактически я ничего не сделал – дерево не посадил, сына не вырастил...»

«Даже когда для других день, я сосредоточен в глубоком колодце своего одиночества, куда редко проникает свет. Ни веревки, ни лестницы внутри колодца нет, а извне о существовании этого самого колодца никто даже и не догадывается, потому что на самом деле никакого колодца нет, есть только сознание, включающее в себя и колодец, и веревку, и лестницу, и чувство глубокого одиночества. Как же это сложно – признаться себе в том, что ты чувствуешь и знаешь, прекратить искать оправдания, а просто принять свою истинную сущность!»

Беседовала Оксана Родионова



## Крис Касперски: «Компьютер как средство решения проблем сам стал одной большой проблемой»

«Системный администратор» № 7-8, 2014 год  
<http://samag.ru/archive/article/2729>

**– Крис, общеизвестно, вы – образцовый трудоголик. Получается, вся ваша жизнь проходит перед монитором?**

– У меня основное время уходит на обдумывание алгоритмов со схематическим изображением квадратиков со стрелочками на бумаге. Вот вам и ответ на вопрос, как не сидеть целый день за компьютером.

Разность ощущений, разумеется, колоссальна. На бумаге значительно меньше знакомств. Даже если брать стандартную консоль (80x25), то нам потребуется целый альбомный лист, а чтобы записать алгоритм в блокноте (не путать с `notepad.exe`), приходится вспоминать крылатое выражение «словам тесно, а мыслям просторно». Иначе мы будем писать исключительно в `write-only`-режиме и потом сами не поймем, что это такое и куда оно работает.

Наверное, поэтому я смутно представляю, зачем нужны IDE и рефракторинг, когда есть FAR и – для полного счастья – `coloreg` (впрочем, на Mac я все-таки использую `TextMate`, но это все же намного ближе к FAR, чем к `Visual Studio`, тем более что FAR с `coloreg` поддерживает сотни языков, как, впрочем, и `TextMate`).

**– Слагают легенды о вашей верности FAR и его известному плагину, также говорят, что с их помощью вы можете практически все...**

– Это не легенды. У меня действительно нет никакого IDE, `coloreg` может не только раскрашивать текст, но и прыгать по парным скобкам, обеспечивает навигацию по функциям (и это еще далеко не все). К тому же он у меня «перепиленный» под себя вдоль и поперек. Вообще у `coloreg` удивительная архитектура, и для расширения функционала даже не обязательно залезать в его исходные тексты.

**– Расскажите о вашем рабочем месте и типичном софте. Сколько у вас компьютеров? Каких?**

– Сейчас у меня в работе два Mac, восемь «виндовых» ноутбуков, стопка «никсовых» серверов, и они укомплектованы обычно следующим образом:

- > Под Win: FAR + `coloreg`, HIEW, OllyDbg, IDA-Pro, Python, MS VC.
- > Под Mac: `TextMate`, `SynalyzeIt`, IDA-Pro, Python, GCC.
- > Под Linux: `vim`, `NetBeans`, IDA-Pro, Python, GCC.

Мой стандартный комплект влезает на флешку и работает на любой системе, включая \*nix и Mac. Компилятор локально не нужен – он стоит за тридевять земель и всегда доступен по `ssh`. Почему некоторые считают `Visual Studio` вершиной прогресса, и, кстати, что это за странное слово «рефракторинг»?



Мой вам совет – *Festina Lente* («поспешай медленно»). Не делай наспех, чтобы потом гарантированно не переделывать. Сначала думай, а потом пиши (программный код), и не пиши заведомо абы как, утешая себя тем, что потом «отрефакторишь». Такой подход формирует привычку, а привычка – это вторая натура.

Впрочем, не нужно заикливаться на инструментарию и любимых компьютерах. К примеру, я выиграл международный конкурс по обфусцированию `JavaScript`, сидя при этом в кафе, где у меня с собой был только телефон `BlackBerry`. Так что не рабочее окружение делает человека. Один хороший знакомый недавно набросал прототип будущей системы и заключил контракт на несколько миллионов долларов на салфетке в таком же прибрежном кафе. Потому что никакой другой бумаги просто не было под рукой. А вот плохому танцору вечно что-то мешает...

**– Вы владеете широким спектром языков программирования. Какова разница между низкоуровневым программированием на ассемблере и на высокоуровневых языках?**

– Грубо говоря, отличие между языками программирования разных уровней как между тактикой и стратегией. При этом многие люди владеют одним из этих умений и немногие – двумя. Я работаю на низком (тактическом) уровне. На уровне архитектуры движка. Рядом со мной работают стратегические архитекторы, потому как движок без колес и руля никому не интересен.

**– Как ассемблерщик и кодокопатель со стажем скажите, есть ли особая романтика у тех ядерных глубин, «куда не ступала нога джависта»?**

– Ядро Linux доступно в исходных текстах, исходные тексты ядра Windows сегодня есть уже практически у всех, кому они нужны, потому для этого совершенно необязательно обращаться к дизассемблеру.

Все это кажется волшебством только до тех пор, пока не понимаешь, как оно работает, но, чтобы не понять, нужно очень сильно постараться. Достаточно лишь прочитать Modern Operating Systems by Andrew Tanenbaum и Windows Internals by Mark Russinovich.

**– Одна из ваших основных специализаций – анализ вирусов и самого разного malware. Вначале были стелз-вирусы, затем пришла эпоха полиморфов, а что потом?**

– ...а потом «замысловатые слова» посыпались как из рога изобилия. Advanced persistent threat (или сокращенно APT) обычно включает в себя сокрытие факта своего присутствия в системе (он же Stealth, он же Root-Kit), активное/пассивное противодействие обнаружению и удалению и т.п.

Полиморфизм – это частный случай метапрограммирования. В computer science под метапрограммированием обычно подразумевают программу, результатом работы которой является другая программа. Пассивные детекторы сканируют файлы в поисках уникальных последовательностей символов. Активные (или как их принято называть проактивные) детекторы работают по принципу поведенческого анализа. Грубо говоря, последовательность вызова API функций – это метрика. Поведенческий анализ распознает определенные сценарии (например, инъекцию кода в доверенный процесс) безотносительно того, как именно они реализованы, и последние несколько лет идут кровопролитные бои за видоизменение поведенческих сценариев до состояния, когда они становятся практически неотличимы от легитимных сценариев популярных программ.

Изменились и угрозы. Если во времена MS-DOS вирусы были «проблемой грязных рук» и не затрагивали тех, кто пользовался лицензионным ПО, то сейчас основная масса вредоносных программ распространяется через документы, эксплуатируя ошибки проектирования.

Дороже всего приходится расплачиваться за ошибки в сетевом стеке. Чтобы подхватить заразу, достаточно всего лишь интернет-подключения, даже браузер запускать необязательно, хотя ошибки в сетевом стеке – большая редкость, и гораздо чаще хакеры проникают через святую троицу – pdf, jar, swf. По умолчанию браузер загружает их автоматически, и, если не установлены обновления, ждите проблем.

**– То есть полиморфическим технологиям сейчас переломили хребет?**

– Отнюдь. Во времена MS-DOS вирусы включали в себя генератор кода, доступный для анализа. Сейчас же код генерируется удаленно на хакерском сервере и отдается по HTTP-запросу. Или... не отдается. Сервер проверяет IP-источник запроса, и в случае каких-либо подозрений последующие ответы возвращают 404 или чистую страницу. К тому же хакеры обязательно проверяют IP на принадлежность к антивирусным компаниям и разным правительственным лабораториям. Да и сам генератор в любом случае остается недоступен. В лучшем случае вы можете его купить на черном рынке за наличные деньги, но чаще всего такая

возможность недоступна, а потому в распоряжении аналитиков есть лишь отдельные экземпляры работы генератора, в которых необходимо выделить неизменную часть, что существенно затрудняет разработку детектора.

К тому же централизованный генератор хакеры могут обновлять так часто, как им вздумается. Прошли времена, когда вирусы работали только под MS-DOS и только под Intel x86. Сейчас необходимо распознавать не только машинный код x86, ARM, PowerPC, не только байт-код (Java, Flash), но и бесчисленное множество скриптовых языков (JavaScript, VBScript, Python). Например, на Mac Python идет предустановленным, что открывает для хакеров новые перспективы. Кстати, Python замечательно распространяется не только в виде скриптов, но и байт-кода.

Мой вам совет – Festina Lente («поспешай медленно»).  
**Не делай наспех, чтобы потом гарантированно не переделывать. Сначала думай, а потом пиши (программный код), и не пиши заведомо абы как, утешая себя тем, что потом «отрефакторишь»**

**– И каковы перспективы традиционного автоматического лечения вирусов?**

– Автоматическое лечение (удаление троянцев) неуклонно сдает свои позиции, и зачастую оно сводится к переустановке системы. Кроме того, лечение возможно только на endpoints. Типичный IPS в лучшем случае предотвращает атаку, но не в состоянии обезвредить уже атакованные системы, поскольку IPS находится между атакуемым и атакующим.

Вообще сейчас у хакера другой приоритет – любой ценой передать управление на свой код, например, расположенный в файле документа и не рассчитанный на исполнение. Эта новая доминанта содействовала развитию веера новых технологий от NOP Slides до Heap-Spray и Return oriented programming (оно же ROP).

**– Как антивирусная индустрия вообще справляется с огромным потоком новых зловредов? Сколько «дохлых тушек», положенных реверсеру на стол, реально обработать за сутки?**

– Этим занимаются специально обученные люди и машины, причем машины все более активно вытесняют людей. Все, что можно автоматизировать, давно автоматизировано. Сейчас этих тушек столько, что никаких человеческих ресурсов на них не хватит. В качестве примера устройства этого процесса могу посоветовать интересную презентацию, ищите ее по ключевым словам: Adobe Malware Classifier.

Вообще дизассемблировать каждую тушку зловреда – это все равно, что хватать вражеских солдат по одному

### Это говорил Крис Касперски

**Первые строки автобиографии на четыре страницы:** «Небрежно одетый мыщър, не обращающий внимание ни на мир, ни на тело, в котором живет, и обитающий исключительно в дебрях машинных кодов и зарослях технических спецификаций».

**О первой написанной игровой программе:** «Нолик и знак «больше» сим-волизировали рыбку, она бегала по экрану взад-вперед, а в центре был рыбак в виде знака вопроса. Чтобы поймать рыбку, нужно было нажать пробел. После рыбки пошли лабиринты. Здесь нужно было рассчитывать алгоритмы, а это уже математика».

**О своих собеседованиях при приеме на работу (в США):** «В России на собеседованиях часто пытаются раздавить, любой ценой показать, что ты ничего не понимаешь – чтобы снизить зарплату. Людей там не ценят так, как деньги. Здесь, в США, чаще всего наоборот: если видят, что ты стоящий специалист, в тебя вцепляются мертвецкой хваткой и больше не отпускают, предлагая лучшие условия на рынке и идя во всем навстречу».

**О жизни и смерти:** «В определенном смысле я никогда не умру, потому что частицы моего Я, мои статьи и книги, разлетелись осколками на века, попав на плодородную почву молодых пытливых умов, изменив ход их бытия, и теперь уже непросто провести границу, где они, а где Я. Во мне живут осколки тех, кто вспыхнул до меня. И так по эстафете. А потому мы приходим к тому, что вначале было слово. Именно слово делает людей бессмертными. Пока кто-то грезит о возможности скопировать свое сознание в компьютер будущего, другие копируют свое сознание посредством письменности».

*Цитаты собрал Владимир Гаков*

и допрашивать. Оно, конечно, полезно. Добыть языка. Одного. А лучше двух. Но что они могут рассказать? Стратегические планы верховного командования им все равно не известны.

Сегодня зловреды – они уже не сами по себе. Они – пушечное мясо на поле кибервойн, сегодня от них зависит чуть больше, чем ничего. Сейчас важно суметь понять устройство хакерской экосистемы – круговорота машинного кода и наличных денег.

**– Вы упомянули о тотальной автоматизации как единственном способе выжить, и я сразу вспомнил о вашем патенте, который получен как раз на тему автоматизации...**

– Было время, работал я удаленно. Ну как работал? Анализировал огромное количество спloitов, причем анализировал медленно, потому что навыка не было. Порядочно устав это делать, я написал программу, которая автоматически сгенерировала другую программу. И вот эта другая программа анализировала спloиты со скоростью один гигабайт в секунду. Запустил ее и улетел в Берген (Норвегия) на встречу со знакомой немкой, с которой у меня тогда был роман.

И когда дней через десять вернулся, программа уже завершала анализ, но у меня хватило ума никому об этом не говорить и до конца года получать «убитых енотов» автоматом. А за пунктуальность и следование намеченным планам на работе мне еще бонусы давали. В конце концов меня заела совесть, и я выслал результаты машинного анализа одним и очень большим куском. В результате эта фирма надолго встала, и теперь мне же пришлось писать еще одну

программу, чтобы автоматизировать труд тех, кто разгребал эти результаты, писал к ним тесты и заносил в базу. Собственно, так я и получил свой первый (и пока единственный) софтверный патент.

**– Перейдем непосредственно к вашей специализации – информационной безопасности. Каковы сейчас самые общие тренды в этой области?**

– Отвечая коротко – основные «тренды» уже сидят, причем сидеть им долго. Лет двадцать, а то и больше. На помощь антивирусам пришли FBI, CIA, US Secret Service и другие страшные слова. Поэтому сейчас маржа везде падает, а посадки растут.

Самый последний писк моды – в прицел атаки попали встраиваемые устройства. В первую очередь это, конечно, роутеры. Зловредный код в роутере очень сложно обнаружить. А тем временем хакеры нашли способ проникнуть внутрь камер наблюдения, подключенных к Ethernet, например, используя процессорные мощности для майнинга биткоинов. На очереди умная бытовая техника (например, холодильники), а также атаки на бортовой компьютер автомобиля – это фантастика новой реальности.

**– Куда идет современный рынок коммерческих решений в области ИБ? Насколько я знаю, это одно из самых быстрорастущих и популярных направлений ИТ?**

– У меня двадцатилетний опыт работы в индустрии безопасности, в том числе и на позиции архитектора. Я хорошо знаю рынок и видел множество примеров успешных начинаний, впрочем, неуспешных примеров было еще больше. Рынок систем безопасности действительно очень быстро растет. И растет он потому, что совсем недавно вирусами занимались школьники, «падонки» и прочие «креативные» личности. Затем персональные компьютеры подключили к банкам, и тут оказалось, что на трояках можно делать деньги.

Рекорд в этом деле – двадцать лет отсидки за шесть доказанных нулей. Накинем еще один ноль за счет недоказанных, но... когда к интернету подключили госучреждения, когда спецслужбы полностью компьютеризировались, внезапно выяснилось, что хакеры – это не просто «оболтусы с Дерибасовской», а угроза национальной безопасности. Сейчас все крупные игроки, ну то есть абсолютно все, купили огромное количество решений безопасности, и на гребне следующей волны пришли системные интеграторы, пытающиеся собрать эту грудку разрозненного баракла воедино.

Но и этот гребень уже пошел на спад, а на горизонте маячит новый, третий. В практическом плане это означает: скоро предстоят сделки на миллионы и миллиарды долларов, но «повезет» здесь только тем, кто к этому уже готов и у кого уже есть готовые решения.

Напомню, что в свое время антивирусы для ПК дали рождение многим нынешним компаниям-миллиардерам, возникшим буквально на пустом месте без каких-либо инвестиций. Но это было относительно давно, в девяностых. Впрочем, суть осталась неизменной – большие деньги зарабатывает тот, кто первым предлагает «спасительную» услугу, когда еще никто толком не осознал своих потребностей и необходимости.



**– Можно ли привести примеры пока не заполненных ниш, чтобы наши читатели, молодые и амбициозные специалисты по ИБ, могли увидеть, где же лежит этот новый и такой вожаемый для многих Клондайк?**

– Что только ни ломают хакеры сегодня. И если на POS-терминале антивирус еще можно представить (хотя с большим трудом), то, например, на surveillance camera антивирус тупо не встанет, потому что это конструктивно не предусмотрено. Хотя де-факто там скорее всего ARM и портированный Linux.

Такая камера вещает потоковое видео, и там хакеры уже нашли дыры, позволяющие заливать шелл-коды со всеми вытекающими последствиями.

Вот мой личный пример из этой оперы. Недавно я прикупил пару Ethernet-камер для своего дома. С камерами идут аккаунты на сервере их производителя с персональным доменом третьего уровня – заходи себе через браузер, введи пароль и смотри удаленно, что там дома у тебя происходит. Два сервомотора обеспечивают свободу наведения, а ИК-подсветка видит даже в темноте – все было бы хорошо, если бы не было так плохо.

Жизнь показала, что эти камеры оказались дырявые, и в них уже поселился ботнет. Сетевым червям даже мозги напрягать не нужно: ваш домен третьего уровня (точка входа в контрольную панель камеры) – это, грубо говоря, число (в данном случае) очень короткое, а потому все камеры сканируются перебором влет и тут же автоматически взламываются. А вот обнаружить такую атаку затруднительно. Ну то есть не то, чтобы совсем затруднительно... Например, если в камере не включен HTTPS, то шелл-коды ловятся sniffером. А если включен? Мне повезло, что в моем случае производитель сделал фейковый HTTPS (ну практически фейковый – у моей камеры нет ресурсов для шифрования видео, и потому по HTTPS она только пароль с логином передает, а все остальное гонит через HTTP).

Поэтому мне пришлось после работы самолично покопаться такую камеру из-за ее заражения, и я обнаружил, что ботнет откликается на определенные http-запросы к камере. Детектор зараженности, быстро написанный мною на «питоне», укладывается меньше, чем в сотню строк. Если накинуть еще пару сотен, то можно на Squid proxy через ICAP-фильтры давить попытки таких червей проникнуть в камеру, заворачивая их «на юг».

Еще личный пример. Видел в местном магазине микроволновку с Ethernet. По сети она сама выкачивает из интернета время и режимы приготовления тех или иных блюд, используя сканер штрих-кода с упаковки товара. От наших электронщиков слышал, что там при старте прошивка грузится в ПЗУ, распаковываясь в память, и что холодный рестарт, возможно, спасет домохозяек. Но что такое холодный рестарт для микроволновки, особенно в США? Если черви будут атаковать потоково, просто устанешь перезагружаться.

Подведем итог: через несколько лет на рынке бытовой электроники будут миллиарды (!) подобных «умных» устройств, подключенных к интернету. Но известные мировые производители бытовой электроники разбираются в безопасности, как «Тузик в апельсинах» (смотрите два моих личных примера выше). И потому они будут вынуждены покупать сторонние решения. Все это огромный, только зарождающийся рынок. И он просто гигантский! Поверьте, что рынок ПК в сравнении с ним «нервно курит в сторонке».

**– Что лично вас восхищает в современных программировании и ИТ, что заставляет двигаться вперед?**

– И вырубает, и восхищает одновременно то, что компьютер как средство решения проблем сам по себе стал одной большой проблемой, и все попытки решения этих проблем лишь порождают новые. Это как на месте срубленной головы Лернейской гидры вырастают две новые.

Беседовал Игорь Савчук



## Статьи, опубликованные впервые в журнале «Системный администратор»

### Технические:

- [1] Глубоководное погружение в чипсет Intel 875P – <http://samag.ru/archive/article/144> (№ 6, 2003).
- [2] Неявный самоконтроль как средство создания неломаемых защит – <http://samag.ru/archive/article/153> (№ 7, 2003).
- [3] Восстановление данных с лазерных дисков – <http://samag.ru/archive/article/161> (№ 8, 2003).
- [4] Могущество кодов Рида-Соломона, или Информация, воскресшая из пепла – <http://samag.ru/archive/article/173> (№ 8, 2003).
- [5] Искривление ТОС как средство борьбы с несанкционированным копированием диска – <http://samag.ru/archive/article/178> (№ 9, 2003).
- [6] Борьба с вирусами. Опыт контртеррористических операций – <http://samag.ru/archive/article/197> (№ 10, 2003).
- [7] Полиномиальная арифметика и поля Галуа, или Информация, воскресшая из пепла II – <http://samag.ru/archive/article/199> (№ 10, 2003).
- [8] Коды Рида-Соломона в практических реализациях, или Информация, воскресшая из пепла III – <http://samag.ru/archive/article/211> (№ 11, 2003).
- [9] Практические советы по восстановлению системы в боевых условиях – <http://samag.ru/archive/article/214> (№ 12, 2003).
- [10] Вирусы в UNIX, или Гибель «Титаника» II – <http://samag.ru/archive/article/223> (№ 1, 2004).
- [11] Жизненный цикл червей – <http://samag.ru/archive/article/249> (№ 2, 2004).
- [12] Ошибки переполнения буфера извне и изнутри как обобщенный опыт реальных атак – <http://samag.ru/archive/article/258> (№ 3, 2004).
- [13] Ошибки переполнения буфера извне и изнутри как обобщенный опыт реальных атак. Часть 2 – <http://samag.ru/archive/article/266> (№ 4, 2004).
- [14] Побег через брандмауэр плюс терминализация всей NT – <http://samag.ru/archive/article/285> (№ 5, 2004).
- [15] Путь воина – внедрение в ре/coff-файлы – <http://samag.ru/archive/article/297> (№ 6, 2004).
- [16] Техника внедрения кода в PE-файлы и методы его удаления – <http://samag.ru/archive/article/315> (№ 7, 2004).
- [17] Разгон и торможение Windows NT – <http://samag.ru/archive/article/327> (№ 8, 2004).
- [18] Восстановление данных на NTFS-разделах – <http://samag.ru/archive/article/342> (№ 9, 2004).
- [19] Восстановление данных на NTFS-разделах. Часть 2 – <http://samag.ru/archive/article/359> (№ 10, 2004).
- [20] Файловая система NTFS извне и изнутри. Часть 1 – <http://samag.ru/archive/article/375> (№ 11, 2004).
- [21] Файловая система NTFS извне и изнутри. Часть 2 – <http://samag.ru/archive/article/395> (№ 12, 2004).
- [22] Как защищают программное обеспечение – <http://samag.ru/archive/article/404> (№ 1, 2005).
- [23] Восстановление NTFS – undelete своими руками – <http://samag.ru/archive/article/414> (№ 1, 2005).
- [24] Техника оптимизации под Linux – <http://samag.ru/archive/article/428> (№ 2, 2005).
- [25] Unformat для NTFS – <http://samag.ru/archive/article/431> (№ 2, 2005).
- [26] Восстановление удаленных файлов под Linux – <http://samag.ru/archive/article/440> (№ 3, 2005).
- [27] Техника оптимизации под Linux. Часть 2. Ветвления – <http://samag.ru/archive/article/449> (№ 3, 2005).
- [28] Техника оптимизации под Linux. Часть 3. Оптимизация циклов – <http://samag.ru/archive/article/465> (№ 4, 2005).
- [29] Восстанавливаем удаленные файлы под BSD – <http://samag.ru/archive/article/474> (№ 5, 2005).
- [30] Насколько неуязвима ваша беспроводная сеть? – <http://samag.ru/archive/article/498> (№ 6, 2005).
- [31] Модифицируем BIOS – <http://samag.ru/archive/article/501> (№ 6, 2005).
- [32] Удаленно управляем BIOS Setup – <http://samag.ru/archive/article/518> (№ 7, 2005).
- [33] CD, не подвластный копированию – <http://samag.ru/archive/article/532> (№ 8, 2005).
- [34] Как спасти данные, если отказал жесткий диск – <http://samag.ru/archive/article/555> (№ 9, 2005).
- [35] Linux/BSD как бастион на пути вирусов – <http://samag.ru/archive/article/565> (№ 10, 2005).
- [36] Антиотладка: старые приемы на новый лад – <http://samag.ru/archive/article/568> (№ 10, 2005).
- [37] Судьба shell-кода на системах с неисполняемым стеком – <http://samag.ru/archive/article/615> (№ 1, 2006).
- [38] Можно ли защититься от переполнения буферов? – <http://samag.ru/archive/article/615> (№ 2, 2006).
- [39] Генная инженерия на службе распаковки PE-файлов – <http://samag.ru/archive/article/673> (№ 5, 2006).
- [40] Техника снятия дампа с защищенных приложений – <http://samag.ru/archive/article/689> (№ 6, 2006).
- [41] Волшебство с паяльником в руках – <http://samag.ru/archive/article/693> (№ 6, 2006).
- [42] Аудит и дизассемблирование эксплоитов – <http://samag.ru/archive/article/721> (№ 8, 2006).
- [43] Упаковщики исполняемых файлов в Linux/BSD – <http://samag.ru/archive/article/731> (№ 9, 2006).
- [44] Как обнаружить malware-программы? Универсальный метод – <http://samag.ru/archive/article/734> (№ 9, 2006).
- [45] Многоядерные процессоры и проблемы, ими порождаемые, в ОС семейства NT – <http://samag.ru/archive/article/1646> (№ 10, 2006).
- [46] Ошибки синхронизации открывают большие возможности для хакеров. Каковы механизмы защиты? – <http://samag.ru/archive/article/1659> (№ 11, 2006).
- [47] Как надо и как не надо защищать веб-контент от кражи – <http://samag.ru/archive/article/1681> (№ 12, 2006).
- [48] Поток аудио/видео с VideoLAN – <http://samag.ru/archive/article/2136> (№ 2, 2008).
- [49] Поиск malware на Server 2003/XP своими руками – <http://samag.ru/archive/article/1590> (№ 3, 2008).
- [50] Жучки в электронных письмах – <http://samag.ru/archive/article/804> (№ 4, 2008).
- [51] Дефекты проектирования Intel Core 2 Duo. Аналитический обзор с точки зрения безопасности – <http://samag.ru/archive/article/809> (№ 6, 2008).

### Общие:

- [52] Рецепты правильного трудоустройства – <http://samag.ru/archive/article/187> (№ 9, 2003).
- [53] Как зарабатывают на Open Source – <http://samag.ru/archive/article/1641> (№ 10, 2006).
- [54] Чего ждать от удаленной работы? – <http://samag.ru/archive/article/1709> (№ 1, 2007).
- [55] Бессистемные заметки о поиске работы за рубежом – <http://samag.ru/archive/article/1670> (№ 5, 2008).