Круговая защита вашего ПК

Казалось бы, не так давно для обеспечения безопасности ПК достаточно было небольшой антивирусной программки. В настоящее время средства защиты приобрели довольно солидные размеры, поскольку их задача — перекрыть все возможные пути попадания вирусов на компьютер. Если раньше основной задачей «вредоносов» было уничтожение данных, то теперь — перехват личной и конфиденциальной информации. Как же защититься от таких угроз?

Сейчас наиболее популярными стали решения класса Internet Security, сочетающие в себе антивирусы, брандмауэры и средства защиты от спама. Основным критерием при выборе антивирусного ПО является качество защиты ПК от угроз. Но не менее важны и такие параметры, как гибкость настроек, скорость работы, продолжительность сканирования ПК на наличие вирусов, скорость реакции вирусных лабораторий на новые угрозы, удобство интерфейса и стоимость программы.

В данной статье мы сравнили шесть наиболее популярных антивирусных продуктов. Поскольку качество антивирусной защиты рассмотренных программ было многократно оценено различными независимыми лабораториями, то в статье будут приведены уже полученные ранее результаты. Критериями же нашего тестирования стали пользовательские характеристики приложений: время, затрачиваемое на установку программы, продолжительность полной проверки системы, загрузка ЦП и ОЗУ при проведении проверки компьютера.

В качестве тестового стенда был использован компьютер с 1,5-ГГц процессором Pentium 4, 1024-Мбайт ОЗУ и предустановленной ОС Windows Vista. На жестком диске было занято примерно 15 Гбайт. По нынешним меркам это довольно слабая модификация, однако новейшие многоядерные компьютеры есть не у всех, а вот защитить свои данные стремится каждый.

Kaspersky Internet Security 2009

В августе прошлого года «Лаборатория Касперского» представила обновленную версию своего антивируса — Kaspersky Internet Security 2009. Этот продукт популярен как в России, так и за рубежом прежде всего благодаря своим широким возможностям по борьбе с вредоносным ПО. Однако эффективность антивирусных программ определяют не только они, но и другие факторы, например скорость работы, загрузка процессора и памяти. В результате нашего тестирования выяснилось, что по скорости сканирования данное решение уступает только Norton Internet Security, а вот по загрузке ОЗУ стоит на предпоследнем месте, обойдя лишь Dr.Web Security Space.

В главном окне программы можно наблюдать за состоянием работы всех компонентов защиты, а также включать, отключать и настраивать их, запускать проверку компьютера на вирусы (быструю или полную), выполнять обновление, просматривать информацию о лицензии.

Продукт KIS 2009 заметно выделяется среди конкурентов большей гибкостью настроек, уступая лишь Eset Smart Security. Он позволяет легко изменять не только уровень обеспечиваемой безопасности, но и методы обнаружения вирусов (использование эвристического анализатора и расширенного поиска руткитов, настройка уровня эвристической проверки, выбор проверяемых объектов, применение технологий iSwift и iChecker), что дает возможность избежать повторного сканирования не изменившихся с момента последней проверки элементов.

Лидерство Kaspersky Internet Security 2009 укрепило и наличие опций, отсутствующих у конкурентов:

■ **Проверка данных, передаваемых по безопасному HTTPS-протоколу.** Для прочтения информации, передаваемой по защищенным каналам, KIS 2009 заменяет запрашиваемый сертификат самоподписанным, что позволяет проверить данные на наличие вирусов.

■ **Виртуальная клавиатура, защищающая от кейлоггеров** — программ, перехватывающих все нажатия клавиш на клавиатуре.

■ **Поиск уязвимостей в ОС и установленном ПО** и загрузка «заплаток».

■ **Анализатор HIPS**, предназначенный для контроля всех запускаемых на компьютере приложений, а также прав каждого из них (ограничение доступа в Интернет, разрешение на использование личной информации и т. п.).

К недостаткам продукта следует отнести значительную загрузку ЦП при первом запуске новых инсталляторов и программ (сказывается влияние анализатора HIPS). При последующих «торможения» не наблюдается. На официальном форуме «Лаборатории Касперского» встречаются жалобы как на невозможность отключить анализатор HIPS, так и на проблемы с обновлением при употреблении не самой последней версии приложения.

Стоимость одной годовой лицензии (на два ПК) Kaspersky Internet Security 2009 составляет 1600 руб., а продление ее на один ПК в течение того же времени будет стоить 960 руб.

Главное окно Kaspersky Internet Security 2009

Norton Internet Security 2009

Выпуская в продажу новую версию Norton Internet Security 2009, компания Symantec обратила особое внимание пользователей на скорость работы продукта: по заявлениям специалистов, установка системы должна занимать меньше минуты. Возможно, этот результат подтвердится на более мощном компьютере. На нашем же тестовом стенде инсталляция заняла 1 мин 52 с. Тем не менее Norton Internet Security 2009 и с таким результатом оказался в разы быстрее своих конкурентов. Лидирует данный антивирус и по скорости сканирования системы, с небольшим отрывом опережая остальных участников. А вот показатель загрузки ЦП у Norton Internet Security оказался не самым лучшим, равно как и требуемый объем оперативной памяти, — за скорость приходится платить.

Программа требует минимум внимания со стороны пользователя, что удобно для начинающих и неспециалистов: после ее установки не нужно производить дополнительных настроек. Автоматическая защита (включенная по умолчанию) на лету проверяет запускаемые файлы, при обнаружении вирусов немедленно удаляет их, помещая копию в карантин, откуда при необходимости файлы можно восстановить.

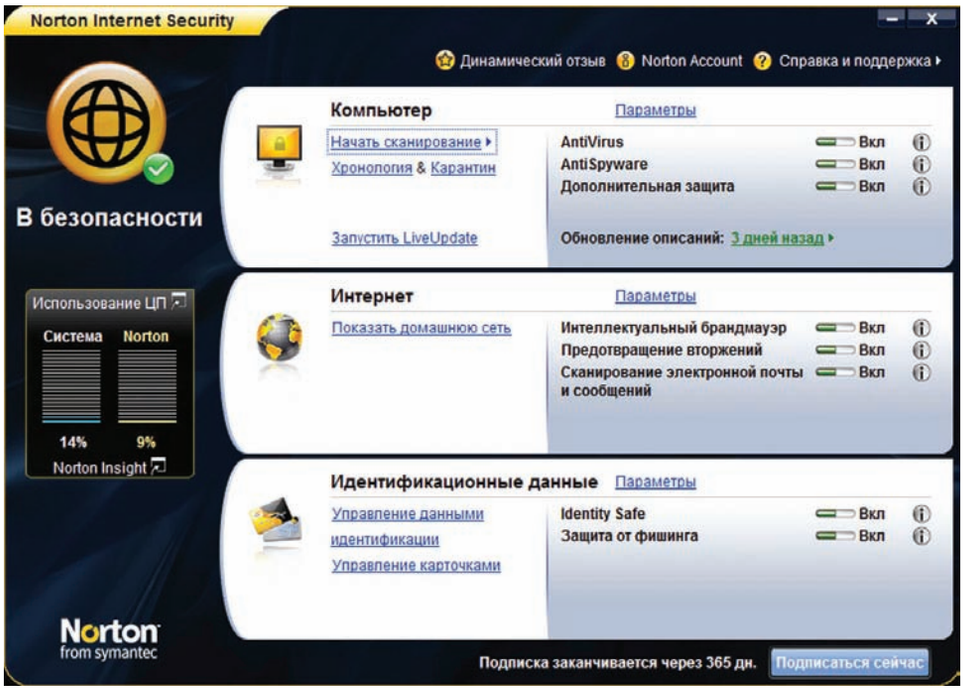
В главном окне можно наблюдать за состоянием всех компонентов защиты, а также включать, отключать и настраивать их. Здесь же представлены статус защиты ПК в целом, использование ЦП системой и программой, информация о подписке.

Из главного окна программы можно запустить сканирование ПК на вирусы, причем предлагается выполнить полную, быструю или выборочную проверку. Все обнаруженные угрозы автоматически удаляются, а их копии помещаются в карантин. Те файлы, которые невозможно удалить (например, с CD-диска), программа относит к категории «Требует внимания» (в случае с CD предлагает извлечь инфицированный носитель).

Результаты тестирований независимых лабораторий

Продукт/ Производитель антивирусного ядра	Разработчик ядра	Уровень детектирования вредоносного ПО по базе VirusInfo[1], место	Тест Anti-Malware на лечение активного заражения[2], место	Тест самозащиты антивирусов от лаборатории Anit-Malware[3], место	Тест на обнаружение вредоносного ПО/ шпионских программ от лаборатории AV-Test	Тест продуктов класса Internet Security от лаборатории AV-Test
«Лаборатория Касперского»/Линейка продуктов Kaspersky 2009	«Лаборатория Касперского»	6	2	2	98,4%/98,3%	11
Symantec/ Линейка продуктов Norton 2009	Symantec	14	3	2	98,7%/92,4%	13
Agnitum/Линейка продуктов Outpost Security Suite	VirusBuster	Н/д[4]	3	2	Н/д	Н/д
F-Secure/ Internet Security,Antivirus 2009	«Лаборатория Касперского»	5	Тест не пройден	4	99,2%/99,6%	13
Eset/Антивирус Eset NOD32, Smart Security,	Eset (ThreatSense)	11	Тест не пройден	4	94,4%/ 94,7%	11
«Доктор Веб»/ DrWeb Antivirus, Security Space 5.0	«Доктор Веб»	Н/д	Н/д	1	84,9%/89,6% (для версии 4.44)	Н/д

[1] За ноябрь 2008 г. [2] За октябрь 2008 г. [3] За январь 2009 г. [4] Н/д — нет данных



Главное окно Norton Internet Security 2009

Полная выгрузка антивируса из памяти не предусмотрена, позволительно лишь отключить либо все, либо отдельные компоненты защиты. Это причинит неудобство пользователям, так как некоторые антивирусные утилиты (например, AVZ, позволяющая уничтожать все известные и неизвестные вредоносные объекты на ПК) требуют полного отключения антивирусного ПО, иначе его драйверы утилита может определить как вирусы.

Есть у Norton Internet Security 2009 и другие отличительные особенности.

■ **Чтобы отражать неизвестные угрозы, антивирус использует расширенную проактивную защиту SONAR,** представляющую собой поведенческий блокиратор.

■ **При посещении сайтов, требующих авторизации, программа предлагает настроить функцию Identity Safe,** сохраняющую учетные записи в специальном защищенном хранилище Norton, что позволяет избежать постоянного ввода персональных данных, защититься от клавиатурных шпионов и перехватов хакерами cookies-файлов, содержащих персональную информацию о пользователе.

По результатам тестирования независимой лаборатории AV-Test продукт вошел в четверку лучших антивирусных решений, эксперты Virusinfo поместили его в середину списка. А вот в тестах Anti-Malware он занял предпоследнее место. Программа уступает конкурентам из-за отсутствия гибких настроек и более низкой скорости реакции вирусной лаборатории на новые угрозы, что значительно повышает риск заражения ПК.

К преимуществам Norton Internet Security относятся удобство интерфейса, повышенная устойчивость к сбоям и незначительное количество ложных срабатываний.

Стоимость годовой лицензии Norton Internet Security на один ПК — 1890 руб., а ее продления еще на год — 1490 руб.

Outpost Security Suite

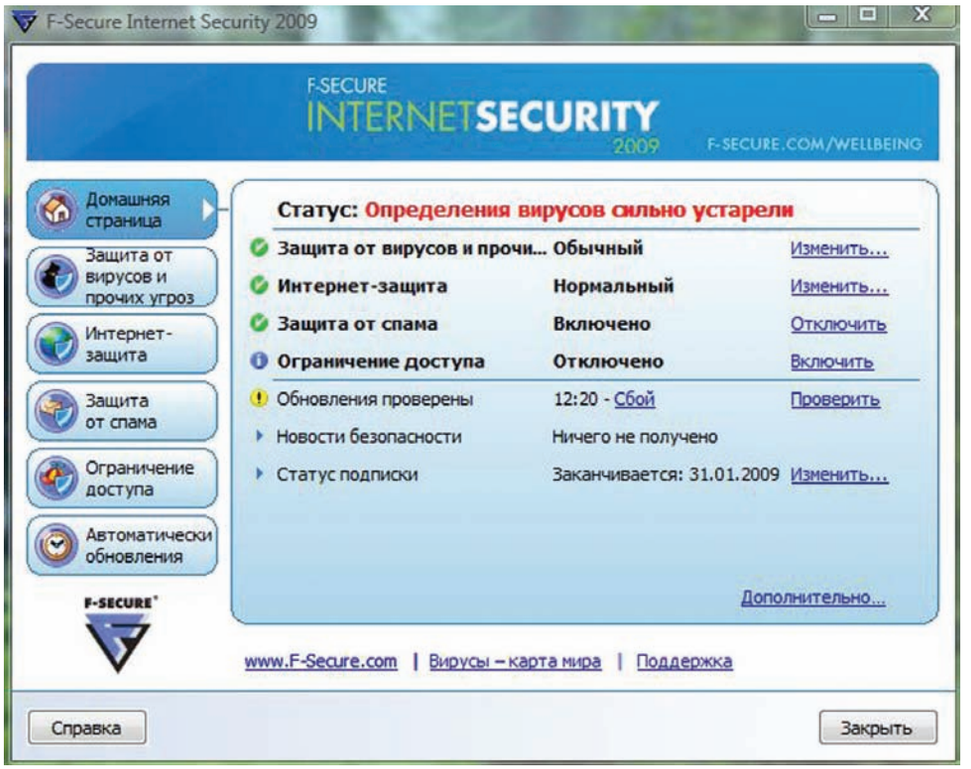
В 2008 г. компания Agnitum выпустила обновленную версию Outpost Security Suite. По функционалу продукт сравним с решением «Лаборатории Касперского», за исключением того, что у него отсутствуют проверка безопасных соединений, виртуальная клавиатура и средства поиска уязвимостей.

Главное окно Outpost Security Suite

В главном окне программы отображаются статус работы всех компонентов защиты (изменение параметров оттуда не производится), информация о состоянии подписки и специальные предложения компании Agnitum, что позволяет запустить обновление и проводить проверку компьютера на наличие вредоносных программ. Кнопка «Настройка», расположенная в правом верхнем углу главного окна, дает возможность изменять многочисленные настройки программы, гибкость которых сравнима только с теми, что есть у Kaspersky Internet Security и Eset Smart Security.

По результатам тестирования лаборатории Anti-Malware, продукт находится в середине списка. Такое положение, по мнению экспертов, связано с тем, что он обнаружил меньше угроз, нежели другие антивирусные решения. Результаты нашего исследования показали, что по таким параметрам, как время установки продукта и полного сканирования ПК, загрузка ЦП и ОЗУ, он не хуже, чем конкуренты, а вот загрузку компьютера значительно замедляет встрроенный анализатор HIPS.

Интегрированный в программу брандмауэр сразу же после установки начинает работать в режиме автообучения, создавая разрешающие правила для всех интернет-соединений. За это разработчикам особое спасибо — они избавили нас, пользователей, от постоянных запросов системы на эту тему. Однако, чтобы такое обучение оказалось успешным, необходимо полное отсутствие на ПК вредоносных программ, иначе и для них могут создаваться разрешающие правила. Чтобы этого не произошло, рекомендуется после установки продук-



Главное окно F-Secure Internet Security 2009

та запустить сканирование ПК на наличие вирусов.

К преимуществам Outpost Security Suite следует отнести гибкость настроек и удобство интерфейса, а также возможность из главного окна программы отправлять подозрительные файлы в вирусную лабораторию.

Годовая лицензия Outpost Security Suite на один ПК стоит 1339 руб.

F-Secure Internet Security 2009

Система F-Secure Internet Security 2009, обеспечивающая полноценную круговую защиту ПК, включает в себя антивирус, антишпион, полноценную защиту в Интернете и родительский контроль.

В главном окне программы, как и у большинства рассматриваемых продуктов, отображаются статус работы всех компонентов защиты с возможностью изменения их параметров, включения и отключения, а также информация о состоянии вирусных баз и подписке. Простота интерфейса — также важное достоинство продукта. Сканирование запускается всего двумя щелчками мыши (на вкладке «Защита от вирусов»), а обновление — прямо из главного окна. Пользователи Vista могут увидеть информацию о статусе защиты компьютера и на боковой панели Windows. Подобная функция предусмотрена только у Norton Internet Security.

Настройки программы достаточно гибкие, но все же в этом она уступает KIS, Outpost Security Suite и Eset NOD32 Smart Security. Нельзя, например, изменять методы обнаружения вирусов, устанавливать уровень эвристического анализатора, варьировать отдельные параметры компонентов защиты (которые всегда включены). Другими словами, тонкую настройку провести не получится.

По мнению экспертов независимых лабораторий Anti-Malware и Virusinfo, продукт входит в шестерку лучших решений, а вот специалисты AV-Test поместили его на 15-е место. До лидирующих позиций ему мешают добраться тяжеловесность и значительное количество ошибок, выдаваемых при работе. В нашем тестировании программа показала наилучший результат по загрузке ЦП. Кстати, загрузка ОЗУ у нее оказалась такой же, как и у KIS 2009, а вот по времени установки она осталась на последнем месте. Большой размер дистрибутива (86 Мбайт) обусловлен наличием в одном установщике сразу двух решений: F-Secure Anti-Virus и F-Secure Internet Security (правда, непонятно, что помешало разработчикам представить их как два отдельных продукта).

К достоинствам F-Secure Internet Security 2009 следует отнести расширенный брандмауэр, позволяющий отслеживать все попытки выхода программ в Интернет, что помогает быстро выявить заражение. Данная опция включена по умолчанию, что также является несомненным преимуществом продукта перед конкурентами.

Увы, не обошлось и без недостатков — при работе выдается большое количество ошибок. За все время тестирования корректно обновить продукт с первого раза так и не удалось.

Лицензия F-Secure Internet Security сроком на год для одного ПК стоит 1998 руб. 63 коп.

Выбор редакции

Лучшая покупка

Сравнительные характеристики комплексных решений для обеспечения безопасности ПК

Продукт	Время установки продукта	Время полного сканирования ПК[1]	Загрузка ЦП при сканировании (среднее значение)	Загрузка ОЗУ при сканировании, Мбайт	Оценка интерфейса[2]
Kaspersky Internet Security 2009	5 мин 30 с	1 ч 20 мин	5%	7	5
Norton Internet Security	1 мин 52 с	1 ч 10 мин	10%	5	5
Outpost Security Suite	4 мин 40 с	1 ч 30 мин	5%	6	4
F-Secure Internet Security 2009	7 мин 50 с	1 ч 40 мин	2%	7	5
Eset NOD32 Smart Security	4 мин	1 ч 30 мин	15%	3	5[3]
Dr.Web Security Space 5.0	4 мин 30 с[4]	6 ч 30 мин	60%	25	3

[1] *Сканирование проводилось при использовании параметров по умолчанию.*

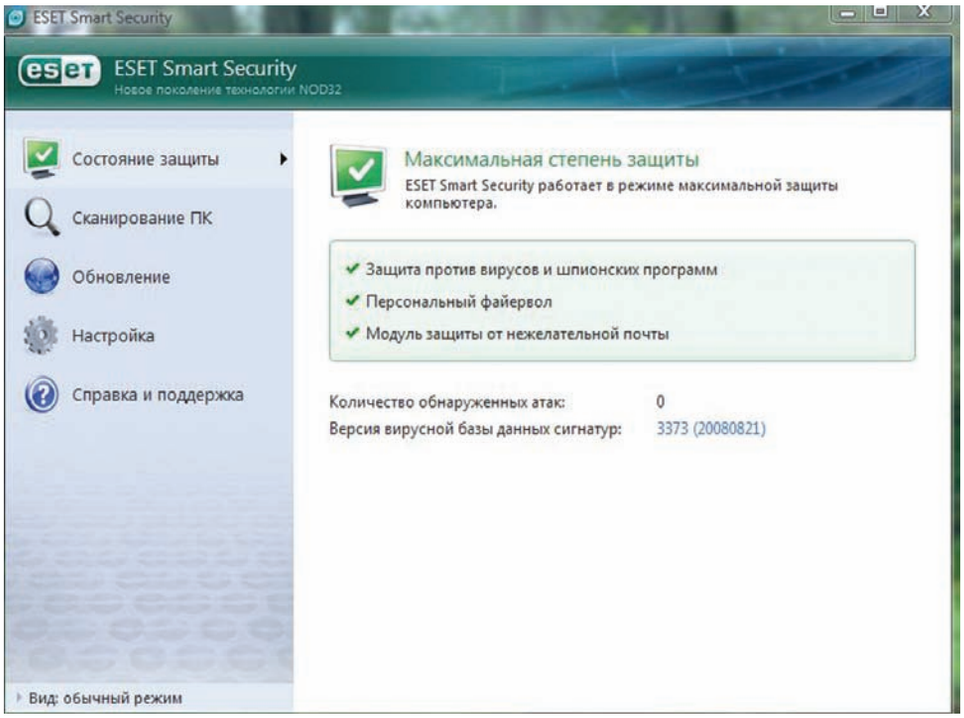
[2] *Оценка проводилась по пятибалльной шкале*

[3] *При использовании расширенного режима* [4] *Без быстрой проверки*

Eset NOD32 Smart Security

В 2008 г. компания Eset представила новую версию своего продукта — Smart Security 3.0, относящуюся к «легким» пакетам защиты ПК. В нашем исследовании он продемонстрировал минимальную загрузку ОЗУ, а вот по загрузке ЦП показал не самые лучшие результаты, обогнав лишь Dr. Web Security Space.

Программа Smart Security предусматривает обычный и расширенный режимы работы. При функционировании в обычном режиме главное окно рассчитано только на просмотр статуса работы всех компонентов защиты. Если же переходить по вкладкам, расположенным на левой панели, можно двумя щелчками мыши запустить обновление антивирусных баз, сканирование компьютера на наличие угроз, а также вызвать окно настроек программы, позволяющих, правда, лишь включать и отключать компоненты защиты, активировать режимы «Блокировать все» или «Пропускать все» для брандмауэра. А вот при работе в расши-



Главное окно Eset Smart Security

ренном режиме в главном окне появляются дополнительные кнопки: «Интерфейс», «Настройка», «Сервис», «Справка». Они предоставляют возможность проводить тонкую настройку программы — изменять виды обнаруживаемых угроз и методы их обнаружения, степень очистки зараженных файлов, просматривать дополнительную статистику, отчеты, карантин, монитор сети и т. д.

По результатам тестирования независимой лаборатории AntiMalware, данный продукт оказался во второй половине списка. Причины тому — еще не реализованное на должном уровне обнаружение активных руткитов, отсутствие поведенческого блокиратора и низкая скорость реакции вирусных лабораторий на новые угрозы.

К положительным сторонам решения следует отнести быстродействие и простоту установки. Кстати, по гибкости настроек оно превосходит конкурентов.

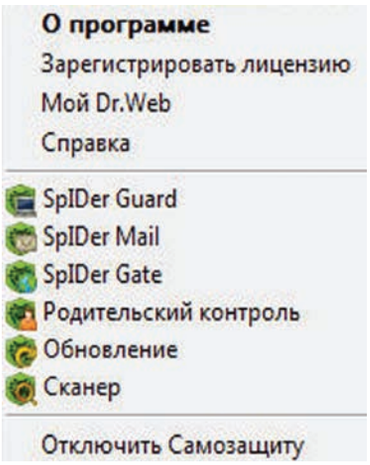
Пакет Eset NOD32 Smart Security поставляется с лицензией стоимостью 1690 руб., действительной для трех ПК.

Dr.Web Security Space

В преддверии нового года компания «Доктор Веб» предложила нашему вниманию новый продукт для комплексной защиты ПК — Dr.Web Security Space. Это один из самых «легких» пакетов, включающий в себя антивирус, антиспам, модуль для проверки HTTP-трафика и родительский контроль.

Главное окно у данной программы отсутствует.

Щелчок правой кнопкой мыши в трее на значке с изображением зеленого паука позволяет включать/отключать компоненты защиты (антивирус, веб-антивирус, почтовый антивирус, родительский контроль и самозащиту), запускать сканирование ПК на наличие вирусов, а также проводить настройку утилиты, используя вкладку «Инструменты». А дважды щелкнув левой кнопкой мыши на том же значке, можно просматривать информацию о программе.



У Dr.Web нет главной страницы, только контекстное меню

Продукт предусматривает возможность более тонко настраивать параметры для безопасной работы в Интернете, включать блокировку тех или иных сайтов, включать/отключать самозащиту.

Его сильные стороны — простота установки, скорость реакции на новые угрозы и гибкость настроек, слабые — слишком длительная проверка на вирусы и значительная загрузка ЦП и ОЗУ.

Впрочем, в целом получился неплохой продукт, но говорить о полной защите ПК пока еще рано.

Стоимость двухгодичной лицензии Dr.Web Security Space для одного компьютера — 1640 руб., причем ее можно продлить на год за 960 руб.

Выводы

Итак, подведем итоги. Лучшую защиту от угроз всех типов обеспечивает Kaspersky Internet Security, однако у программы не самые высокие показатели по быстродействию (особенно при запуске новых программ и инсталляторов). К наиболее простым в эксплуатации решениям следует отнести Norton Internet Security и Dr.Web Security Space.

Продукт Norton Internet Security обладает достаточно широкими функциональными возможностями, но в отличие от Dr.Web здесь отмечается более низкая скорость реакции лабораторий на новые угрозы.

А программа Dr.Web в свою очередь не отличается «скорострельностью» проверки на вирусы.

Решение F-Secure характеризуется достаточно высокой скоростью реакции вирусных лабораторий на новые угрозы и широкими функциями брандмауэра, но, к сожалению, у него возникают сбои во время работы.

Продукт Outpost Security Suite имеет примерно такие же настройки, что и KIS, но скорость реакции у него гораздо ниже, что повышает риск заражения.

Программа Eset NOD32 Smart Security обладает хорошей гибкостью настроек, но довольно низкой скоростью реакции вирусных лабораторий на новые угрозы. ●

— Евгений Шахов

Лучшим решением среди всех рассмотренных был признан антивирус Kaspersky Internet Security 2009, обеспечивающий самую высокую степень защиты от угроз всех типов. Ему достается «Выбор редакции». «Лучшей покупкой» признан Eset NOD32 Smart Security, включающий сразу 3 лицензии за умеренную плату.

Мария Сысойкина

Официальная бета-версия Windows 7

Сразу после новогодних праздников компания Microsoft преподнесла всему миру долгожданный подарок — официальную бета-версию новой операционной системы Windows 7. Как уже сообщалось, появившаяся ОС базируется на нынешней Vista, однако имеет усовершенствованную систему контроля действий пользователя, улучшенные элементы интерфейса, повышенное быстродействие и отличается ускоренной загрузкой.

Желающих познакомиться с новой ОС оказалось так много, что 9 января, в день открытия полного доступа к бета-версии, серверы Microsoft не выдержали нагрузки. Многим пользователям пришлось загружать дистрибутив через файлообменники. Надо сказать, что даже сами сотрудники Microsoft не ожидали такого ажиотажа.

Буквально через несколько дней разработчикам Microsoft пришлось выложить в Сеть первый патч к Windows 7, поскольку энтузиасты помогли обнаружить ошибку при работе с MP3-файлами. Оказывается, в случае редактирования довольно большого количества метатегов в таких файлах из записи пропадает несколько секунд звука. Кстати, ошибка возникает и без вмешательства пользователя, например тогда, когда медиапроигрыватель подгружает теги из Интернета. Воспользовавшись случаем, разработчики включили в патч и критически важное исправление для более старых операционных систем, устраняющее серьезную уязвимость в протоколе обмена файлами SMB.

Напомним, что выход окончательной версии Windows 7 ориентировочно запланирован на конец этого года.

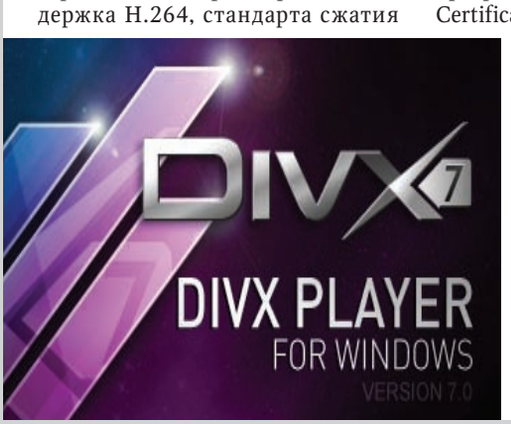
DivX 7

Компания DivX представила новую версию одноименного продукта, которая может заинтересовать как любителей, так и профессионалов в области цифрового видео. Теперь пользователям Windows стал доступен пакет DivX 7, выпущенный в двух редакциях. Бесплатная версия предназначена лишь для воспроизведения файлов, а версия DivX Pro содержит инструменты для создания видео.

Ключевая особенность новой версии кодека — расширенная поддержка H.264, стандарта сжатия видео, отвечающего за воспроизведение видео высокой четкости. При этом обеспечивается работа с файлами, имеющими разрешение до 1080p.

Поддержка HD-видео не только осуществлена на уровне кодека, но и включена в дополнительные утилиты. Так, новый конвертер файлов из пакета DivX 7 способен преобразовывать видеофайлы в формат DivX Plus, базирующийся на стандартах H.264 и AAC. Разработчики прочат новому формату большое будущее, они даже запустили специальную программу сертификации DivX Plus Certification. В результате производители оборудования смогут реализовать поддержку нового формата в собственных продуктах, например в проигрывателях DVD и Blu-ray. Вероятно, первые устройства, сертифицированные для работы с форматом DivX Plus, появятся уже к концу года.

Как и раньше, в пакет DivX 7 включен проигрыватель, понимающий и файлы формата mkv.



Maxthon 2.5

В середине января увидела свет свежая версия легкого и производительного браузера Maxthon 2.5.

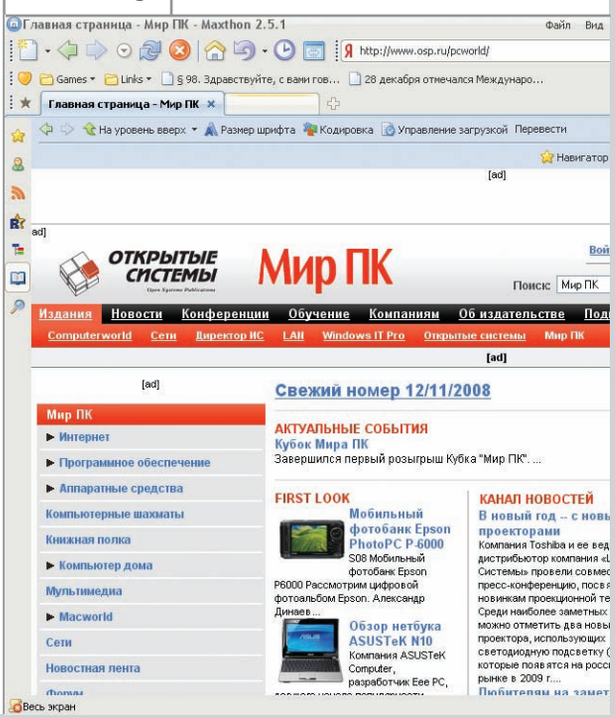
Базируется Maxthon на ядре Internet Explorer, однако имеет более гибкий интерфейс и более широкие настройки, нежели его собрат.

В данной версии пользователям стали доступны новый механизм блокировки всплывающих окон, а также возможность анонимно посещать веб-страницы.

При первом запуске программа наряду со стандартным вопросом о браузере по умолчанию предложит пользователю настроить собственный аккаунт для сохранения личных настроек. Количество всевозможных настроек возможностей браузера действительно поражает. Нажатием одной кнопки в меню можно отключить загрузку изображений, флэш-объектов, Java-аплетов, а затем просмотреть список отключенных объектов. Браузер позволяет подогнать по ширине экрана страницы с длинными строками или большими картинками, чтобы избежать горизонтальной прокрутки. Удобным покажется и вертикальное служебное меню, где располагаются кнопки управления закладками, поиском, встроенным RSS-модулем.

Пожалуй, единственная проблема браузера в том, что такое количество функций придется слишком долго запоминать. Видимо, поэтому минималистский Google Chrome, например, гораздо быстрее завоевал популярность пользователей.

Браузер распространяется бесплатно, по лицензии GNU GPL.



Под колпаком

Интернет давно стал неотъемлемой частью нашей жизни как дома, так и на рабочем месте. Порой проще написать человеку сообщение по «аське», чем позвонить по телефону, или скинуть пару рабочих файлов по почте, чем переносить их на флэшке. Но мало кто, выполняя эти операции, ставшие уже рутинными, предполагает, что его действия могут создавать угрозу компании.

Конечно, постфактум отдельные пользователи начинают беспокоиться. На форумах и в блогах часто всплывают вопросы о том, как узнать, не читают ли третьи лица почтовые сообщения и не станет ли личная информация доступна службе безопасности предприятия? Ведь есть же оригиналы, которые умудряются писать романтические послания с корпоративных почтовых адресов. А уж как любят в компаниях стращать новых сотрудников! Ну кто из вас не слышал такого: «У нас всю почту читают, «аську» прослушивают, так что лучше ничего личного не пиши»?

Чтобы развеять сомнения переживающих пользователей, мы проконсультировались со специалистами LETA IT-company, занимающимися внедрением систем защиты от утечки данных.

Ничего личного

По имеющейся статистике, более половины организаций, внедривших DLP-системы (Data Leak Protection — система защиты от утечки данных), информируют своих сотрудников о подобном контроле. Но если у вас все же возникли подозрения, не стоит особо волноваться. Во-первых, такие системы недешевы, и потому даже простой по функциональности вариант может позволить себе далеко не каждая компания. Во-вторых, они предназначены вовсе не для того, чтобы подглядывать за работниками. Цель DLP-решений — контролировать утечки внутрикорпоративной информации, секретных сведений и проч. Так что если вы не «сливаете» конкурентам клиентскую базу, а всего лишь рассылаете с рабочего адреса приглашения на вечеринку, вам не о чем беспокоиться.

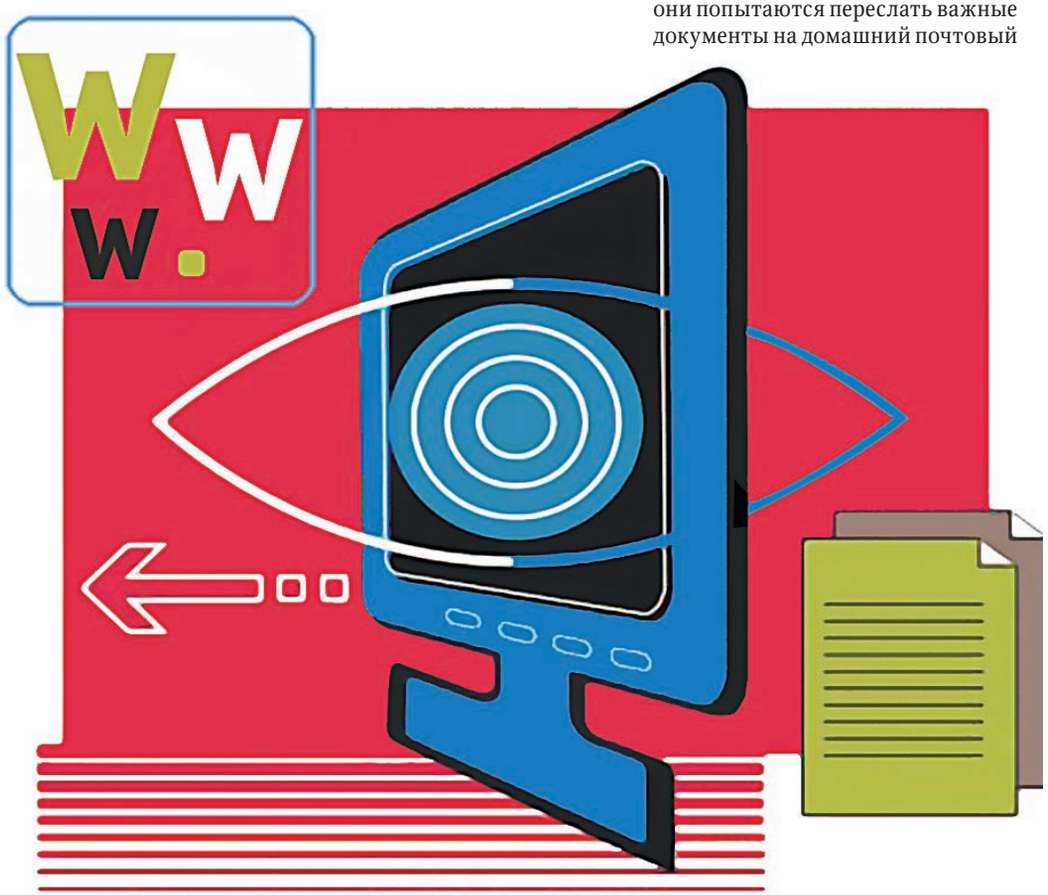
Внедряя DLP-систему, компании, как правило, руководствуются следующими целями :

- уменьшить финансовые потери от разглашения конфиденциальной информации;
- избежать репутационных рисков, также имеющих денежное выражение;
- соответствовать отраслевым стандартам безопасности (характерно для западных компаний).

Взвесив возможные угрозы, компания выбирает подходящее для себя решение, причем приоритеты в защите расставляются примерно так. Всегда и обязательно устанавливается контроль за корпоративной почтой, во вторую очередь — за интернет-трафиком (бесплатные почтовые серверы, форумы, блогоплощадки и проч.) и интернет-пейджерами. А вот контролю посредством DLP-системы за сетевыми принтерами и USB-портами уделяют внимание далеко не все фирмы. Как правило, принтеры в помещениях находятся на виду, и не каждый рискнет открыто распечатывать, например, бизнес-план нового проекта или подробности последнего крупного контракта. А вот то, что на рабочих станциях отказываются от контроля USB-портов и записывающих устройств, имеет свое объяснение. Для функционирования таких систем требуется установить специальное ПО на компьютере пользователя, а значит, подобный вариант не подходит компании, если она хочет сохранить в тайне факт контроля, .

А каковы же мотивы сотрудников, чью неправомерную деятельность отследила DLP-система? Как ни странно, большинство случаев связано непосредственно с выполнением служебных обязанностей, а вовсе не с подрывными действиями. Так, многие трудолюбивые сотрудники часто берут работу домой, заканчивая срочные дела в выходные или по ночам. Так вот, когда они попытаются переслать важные документы на домашний почтовый

Цель DLP-решений — контролировать утечки внутрикорпоративной информации, секретных сведений и проч. Так что если вы не «сливаете» конкурентам клиентскую базу, а всего лишь рассылаете с рабочего адреса приглашения на вечеринку, вам не о чем беспокоиться



адрес или скопировать эти файлы на флэшку, система уведомит о произошедшем кого нужно и наутро таких деятельных товарищей ждут долгие объяснения с начальством. Кроме того, если важные сведения случайно или по чьей-либо просьбе будут отправлены на сомнительный адрес (например, на бесплатный почтовый сервер), система также забьет тревогу.

Иногда сотрудники компании преследуют и карьерные цели, пытаясь, например, при переходе на новое место работы или в случае кризиса прихватить с собой часть клиентской базы. Но, конечно, самыми опасными для компании являются ситуации, когда сотрудник просто продает информацию конкурентам или передает злоумышленникам.

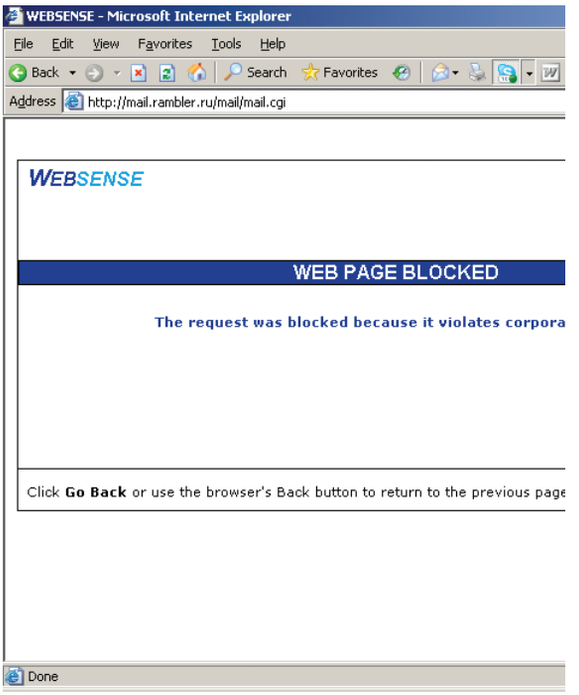
Сверим отпечатки

Работа системы контроля утечки информации может базироваться на одном из двух методов. Первый, называемый методом цифровых отпечатков, более сложен, но и значительно эффективнее. Второй, основанный на использовании ключевых слов, более прост, однако не всегда точен.

В первом случае системе дается некий массив документов, на котором она «обучается». При этом тексты лучше классифицировать по группам: финансовая отчетность, интеллектуальные разработки и т. д.

Система запоминает «цифровые отпечатки» содержания документов, а затем, сканируя поток исходящей информации, определяет, присутствуют ли в нем фрагменты конфиденциальных данных. Если в теле письма или приложенном файле найдено совпадение, система формирует инцидент — отправляет офицеру безопасности сообщение, в котором указано, кто кому и что отправил. Причем в отчет включены все сведения об исходном конфиденциальном документе — к какой группе информации он относится, где физически размещен файл и т. д.

Когда система обнаруживает подозрительное письмо,она либо только информирует владельца сведений или сотрудника службы безопасности, либо блокирует сообщение до проведения полной проверки его содержания. В такой ситуации решение остается за офицером СБ. Если он решит, что в письме не содержится конфиденциальных данных, то может разрешить его отправку адресату. Так, например, если бухгалтер посылает финансовый отчет, система обязательно обнаруживает попытку перемещения данных. Однако если это правомерная, но неизвестная DLP-системе отправка (например, в налоговую инспекцию), то для разблокирования письма потребуется вмешательство ответственных сотрудников.



Вот что система выдает пользователю при отправке подозрительного письма

Обмануть невозможно

Можно ли обмануть систему контроля утечек информации? Практически нет.

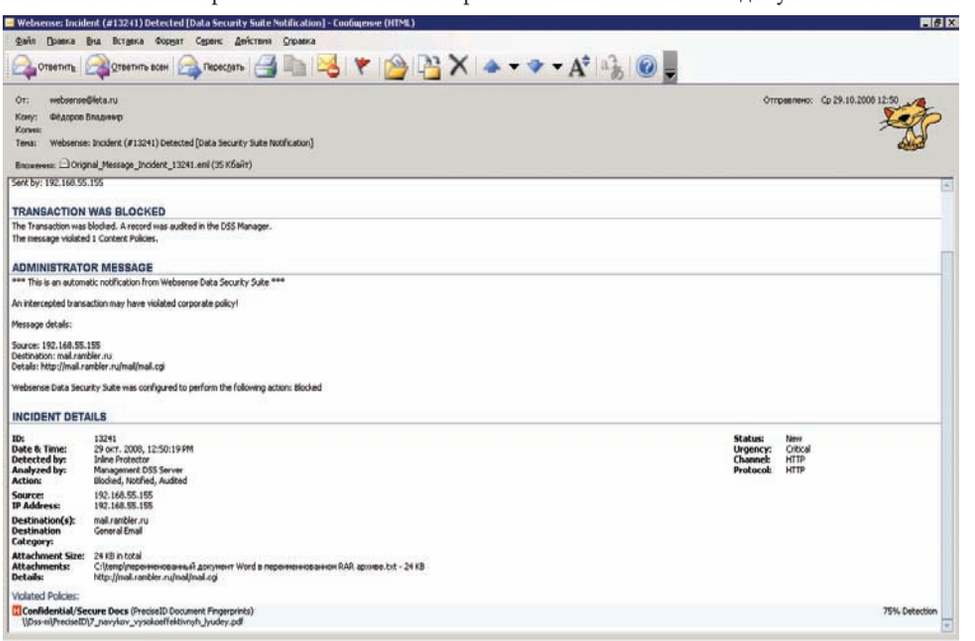
В качестве эксперимента мы попробовали отправить фрагмент конфиденциального документа через сеть, контролируемую системой Websense Data Security Suite по методу цифровых отпечатков. Однако, прежде чем отправить текст, мы произвели с ним несколько действий. Сначала вставили нужный нам фрагмент в большой файл электронной книги. Затем переименовали файл, присвоив ему расширение MP3. Потом запаковали документ в RAR-архив и снова изменили расширение на TXT. В таком виде мы попытались отправить файл с почтового ящика на почтовом сервере Rambler. Казалось бы, система ни за что не поймет, что мы посылаем. Но не тут-то было! Сообщение не было отправлено, а в службу безопасности пришло соответствующее письмо с полным указанием всей информации об отправляемом файле, отправителе, получателе и даже об исходном документе, фрагмент которого мы пытались похитить.

Система «засечет» хищение и в том случае, если вставить текст в слайд презентации или PDF-файл. Не поможет даже такой способ, как замена кириллических символов латиницей. Система все равно обнаружит инцидент и сообщит, что отправляемый документ похож на исходный, однако с ним были проделаны какие-то манипуляции.

Теоретически документ можно зашифровать. Но система легко определяет использование штатных средств шифрования, поэтому злоумышленнику придется изобрести собственный шифр, чтобы изменить текст до неузнаваемости и обвести систему вокруг пальца.

В ближайшем времени производители DLP-систем планируют внедрить даже такую функциональность, как распознавание текста в сканированных документах. Осталось лишь решить вопрос с производственными мощностями, поскольку работа OCR-компонента станет большой нагрузкой на сервер.

С помощью DLP также можно контролировать, например, запись важных документов на внеш-



А это система сообщает сотрудникам СБ при отправке пользователем подозрительного письма

Как это работает?

Конечно, если злоумышленник просто перескажет в письме нужные сведения своими словами, метод цифровых отпечатков может и не сработать. В этом случае подойдет метод с применением ключевых слов. На практике он используется редко, так как набор нужных фраз сложно поддерживать в актуальном состоянии, и значит, возможен большой процент ложных срабатываний системы. Чаще ключевые слова применяют лишь для мониторинга, т. е. система просто фиксирует наличие определенных фраз в сообщении, но не блокирует отправку.

ние носители. Однако это требует установки на клиентские компьютеры дополнительных приложений и базы данных цифровых отпечатков. А чтобы не загружать рабочую станцию, базу отпечатков приходится сильно урезать, из-за чего снижается эффективность проверки. В подобной ситуации можно либо установить блокировку USB-портов, либо контролировать доступ к важным файлам.

Для недоверчивых

Если же вы до сих пор волнуетесь из-за того, что ваша неделовая корреспонденция может попасть в чужие руки, спешим уверить вас в обратном. Вряд ли серьезная компания будет приобретать и использовать такие решения, чтобы знакомиться с личной перепиской сотрудников. Конечно, автоматизированная система просматривает всю информацию, однако в службу безопасности компании попадает лишь то, что так или иначе создает угрозу нарушения коммерческой тайны.

Что же касается опасений о просмотре писем вручную, то, во-первых, это довольно трудоемкий процесс, во-вторых, не совсем легальный. В российском законодательстве есть несколько не вполне согласованных положений на сей счет, и потому очень сложно доказать, что проводился неавтоматизированный просмотр, даже если с сотрудником и был подписан договор о неразглашении коммерческой тайны.

В целом, если вы не хотите попасть в неловкое положение, старайтесь осторожно использовать информационные ресурсы компании и не допускать утечек информации.

Напоследок мы приводим несколько рекомендаций, предложенных Николаем Зениным, руководителем направления защиты коммерческих тайн LETA IT-company. Они помогут избежать «случайных» конфликтов с системами контроля информации и корпоративными службами безопасности, возникающих по незнанию и неосторожности:

- не отсылайте на непроверенные адреса важные документы компании;
- не прикладывайте к личной переписке документы, составляющие коммерческую тайну компании;
- снабжайте исходящую из компании корреспонденцию такими комментариями, которые не стыдно было бы показать службе безопасности;
- не оставляйте в течение продолжительного времени распечатанные конфиденциальные документы на принтере или открыто на рабочем месте;
- не злоупотребляйте корпоративным Интернетом (если более половины посещаемых вами интернет-сайтов явно не связаны с выполняемыми служебными обязанностями, это может вызвать лишние вопросы у контролирующих сотрудников).●

— Мария Сысойкина

Внимание всем портам!

С развитием техники компании подвергаются все большим рискам: сотрудники чаще копируют данные с рабочего ПК на внешние диски или в личные КПК и коммуникаторы, а также больше документов распечатывают на корпоративных принтерах. При этом не исключено, что таким образом за пределы офиса могут быть вынесены сведения, представляющие коммерческую тайну.

Конечно, в целях эффективного развития компании службе безопасности лучше разрешить доступ к таким устройствам, но тогда нужно обеспечить надежный контроль над данными, которые могут быть записаны, переданы или распечатаны.

Сейчас существует несколько решений, позволяющих контролировать работу внешних устройств и портов на рабочем компьютере пользователя. Один из подобных комплексных продуктов — DeviceLock 6.3, контролирующий помимо всего прочего такие потенциальные каналы утечки данных, как смартфоны и КПК, USB-устройства и принтеры.

Функция блокировки или контроля USB-портов стандартна для многих решений, однако DeviceLock поможет обезопасить компанию от утечек посредством шифрования данных, переносимых на внешние устройства хранения. Для этого в программу включена интеграция с внешними криптографическими продуктами, позволяющими шифровать флэшки целиком, а также DeviceLock распознает флэш-диски с аппаратным шифрованием.

По мнению многих пользователей, вся потенциально полезная в работе информация должна быть синхронизирована с мобильным устройством — КПК, смартфоном, коммуникатором, подключенным через порты USB, COM или IrDA, по интерфейсам Bluetooth, Wi-Fi. Таким образом, в памяти смартфонов оказываются данные календаря Outlook, полная копия почтовых сообщений, контакты, разного рода файлы, заметки, задачи и т. п. Вряд ли сотрудник , копирующий корпоративную информацию, задумается о том, к чему может привести кража или потеря КПК. В последней версии DeviceLock реализован контроль мобильных устройств на базе Windows Mobile и Palm OS. Благодаря этому функционалу служба информационной безопасности получила возможность выборочно разрешить или запретить обмен данными календаря, контактов, почтовых сообщений и в том числе связанных с ними файлов, заметок и задач. Специальная опция теневого копирования позволяет сохранить в базе данных переданные на мобильные устройства сведения, а затем проанализировать их.

Не стоит забывать и о таком на первый взгляд безвредном канале утечки, как печать. Контроль процессов печати в корпоративной среде — ключевая особенность версии DeviceLock 6.3, позволяющая администраторам централизованно следить за доступом пользователей к локальным, сетевым и виртуальным принтерам, причем независимо от способа их подключения к компьютерам. DeviceLock 6.3 позволяет для каждого отдельного компьютера в сети, для их групп, для всех компьютеров подразделения или же для полного их парка в организации задать правила доступа, определяющие, кому, когда и на каких принтерах разрешено печатать. Причем такие правила можно определить для отдельных пользователей, для их групп, для департаментов или же сразу для организации.

Delphi Prism — работаем с файлами

Решение более-менее серьезных задач обычно требует длительного хранения информации — настроек программы, истории работы и т. д. Этим объясняется постоянный интерес к теме работы с файлами. Платформа .NET имеет все необходимое для того, чтобы программист забыл про существование устройств хранения данных и полностью довериться «матрице» — мощной объектной модели.

Получив такой инструмент, как Delphi Prism, многие «дельфисты» обрели полноценный доступ к технологиям самой последней версии платформы .NET. Конечно, если сравнивать новый продукт, например с C#, наверняка в нем пока будет чего-то не хватать, однако сам факт выхода Delphi Prism, кажется, решает проблему постоянного отставания Delphi.NET от поддержки широкого набора средств работы под .NET и Mono.

В настоящее время все тонкости работы в новой среде программирования можно условно разделить на относящиеся к употреблению пока еще непривычного для большинства «дельфистов» синтаксиса и на касающиеся свежих возможностей самой платформы .NET.

Особенности платформы .NET

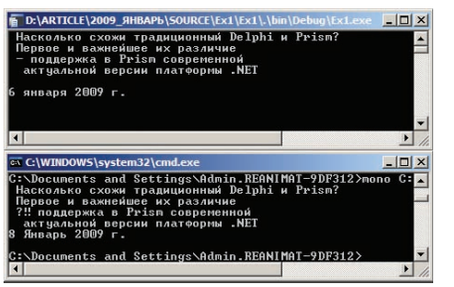
Когда речь заходит о работе с файлами на платформе .NET, то на первое место сразу же выступает тема использования асинхронных потоков данных, точнее, даже не самих потоков, а классов-оберток, которые обеспечивают программисту рутинные операции.

Отдельно стоит упомянуть класс File (System.IO.File). В нем собраны многие возможности по работе с файловой структурой. Для его использования требуется .NET Framework 3.5 — современная версия .NET, поддерживаемая Delphi Prism. С нее-то мы и начнем.

Сначала в первом примере просто создадим новый файл с помощью волшебного класса File.

Листинг 1. Чтение текстового файла с использованием классов File и StreamWriter

```
namespace Ex1;
interface
uses System.IO;
type
  ConsoleApp = class
  public
    class method Main;
  end;
implementation
 class method ConsoleApp.Main;
begin
// Создание текстового файла
// и запись в него данных
var filename:="C:\Ex1.txt";
 using tr:StreamWriter:=File.
CreateText(filename) do begin
    tr.WriteLine("Насколько схожи \
      традиционный Delphi и Prism?");
    tr.WriteLine(" Первое и важнейшее \
      их различие");
    tr.WriteLine(" – поддержка в Prism со-
временной");
    tr.WriteLine(" актуальной версии плат-
формы .NET");
 end;
//Вывод в консоль содержимого файла вместе
//с датой создания
//Чем-то похоже на FileToString из JEDI для
//Delphi
   Console.WriteLine(File.
ReadAllText(filename));
   Console.WriteLine((new FileInfo(filename)).
CreationTime.ToLongDateString);
      File.Delete(filename);
   Console.ReadKey;
end;
end.
```

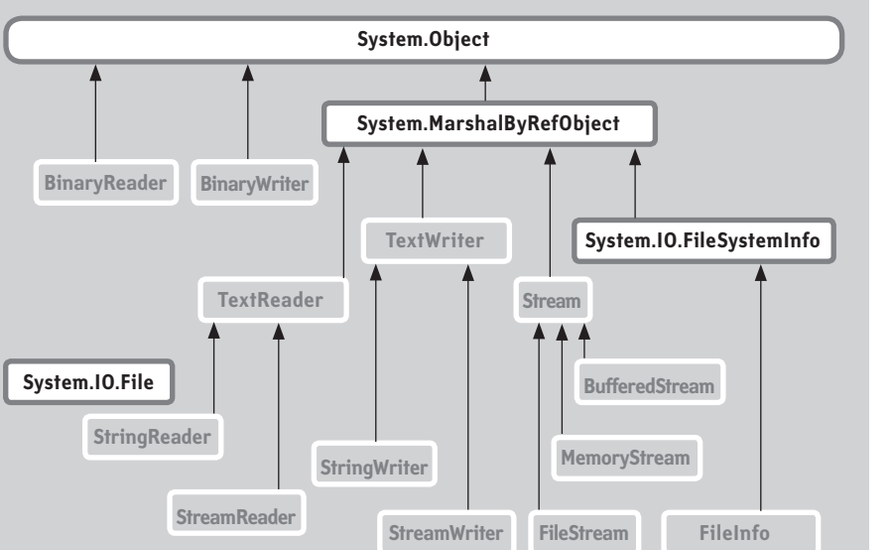


Класс StreamWriter предназначен специально для записи текстового файла. При этом мы почти до предела упростили для себя работу, используя конструкцию using ... do begin ... end; Она заменяет конструкцию

```
try
finally
    if (_Object is Idisposable) then (_
Object as Disposable).Dispose();
end;
```

где _Object — условное обозначение создаваемого объекта. Таким образом, программист частично снимает с себя ответственность за жизненный цикл созданного объекта независимо от модели его памяти. Напоследок упомянем FileInfo — еще один волшебный класс, сопоставимый по

Фрагмент иерархии классов, связанных с потоками из пространства имен System.IO



Более полная информация по иерархии классов имеется на сайте http://msdn.microsoft.com/ru-ru/library/default.aspx

мощности с классом File. Оба они предназначены для решения одних и тех же задач, но для FileInfo нужно создавать экземпляр класса.

StreamWriter и StreamReader — классы, специально созданные для работы с текстом. Конечно, желательно, чтобы вы были уверены, что будете работать именно с текстом, в противном случае рекомендуется выбрать класс FileStream. Классы StreamWriter и StreamReader освобождают программиста от забот, связанных с кодировкой. Поразительно, насколько все кажется в .NET взаимозаменяемым и универсальным!

Теперь напишем еще более скромную программу для чтения файла EMPLOYEE.txt, использовав класс StreamReader. Сначала экспортируем таблицу EMPLOYEE.FDB (из демонстрационной базы для пакета FireBird 2.0) в текстовый файл. В качестве разделителя зададим символ «;». В результате получим полноценный CSV-файл, с которым можно упражняться.

Листинг 2. Чтение текстового файла EMPLOYEE.txt с использованием класса StreamReader

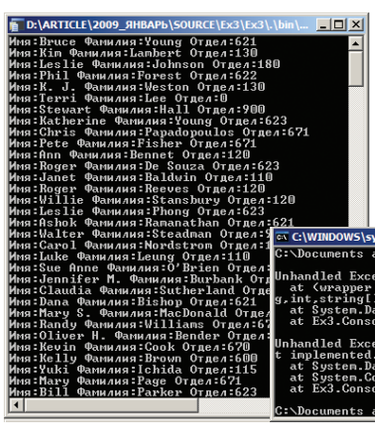
```
…
class method ConsoleApp.Main;
begin
  //Для чтения текстового файла применим
//класс StreamReader
  using tr: StreamReader:=new
StreamReader("C:\EMPLOYEE.txt") do begin

      loop begin

          var line:=tr.ReadLine ;

          if not(Assigned(line)) then
break;

          Console.WriteLine(line);

        end;
      Console.ReadLine;
    end;
  end;
end.
```

Рассмотрим второй пример. Вместо строки

```
tr:StreamReader:=new StreamReader("C:\
EMPLOYEE.txt")
```

можно просто написать

```
tr:=new StreamReader("C:\EMPLOYEE.txt")
```



Полученная конструкция также будет работать. Обратите внимание: если вместо конструктора StreamReader поставить родительский конструктор TextReader и явно указать тип StreamReader для идентификатора tr, то компилятор и это верно расценит.

Простым чтением собственного файла никого не удивить, поэтому добавим элементы анализа данных, т. е. поставим задачу разбора полей.

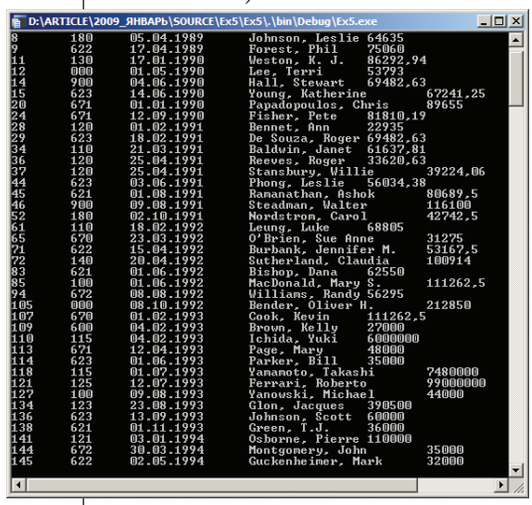
Листинг 3. Применение технологии OLEDB для чтения и анализа данных текстового файла

```
…
class method ConsoleApp.Main;
begin
//Читаем текстовый файл с использованием
//технологии OLEDB
    var FileName:='C:\EMPLOYEE.txt';
    var Delimited:=';';
    var file:FileInfo:=new
FileInfo(FileName);

  using  con:OleDbConnection:=
           new OleDbConnection(
         'Provider=Microsoft.Jet.
OLEDB.4.0;Data Source='+
         file.DirectoryName+
         ';Extended Properties=''tex
t;HDR=Yes;FMT=Delimited('+
         Delimited
         +')'';') do begin

       con.Open();

       using cmd:OleDbCommand:=new
OleDbCommand(string.Format ("SELECT *
FROM [{0}]", File.Name), con) do begin

       using rdr:OleDbDataReader:=cmd.
ExecuteReader() do begin

                while (rdr.Read()) do begin

  //Выборочно выводим столбцы в консоль
  Console.WriteLine('Имя:{0} Фамилия:{1} Отдел
:{2}',rdr[1],rdr[2],rdr[5]);

                end;

                rdr.Close;

            end;
          Console.ReadLine;
          end;
        end;
    end;
end.
```

В третьем примере была использована технология работы с базами данных без самой базы. Конечно, можно решать задачу в лоб, используя основные возможности платформы .NET, — применить метод класса String.Split, который автоматически будет разбивать очередную читаемую строку на элементы и заносить их в массив, но, согласитесь, что вышло оригинально.

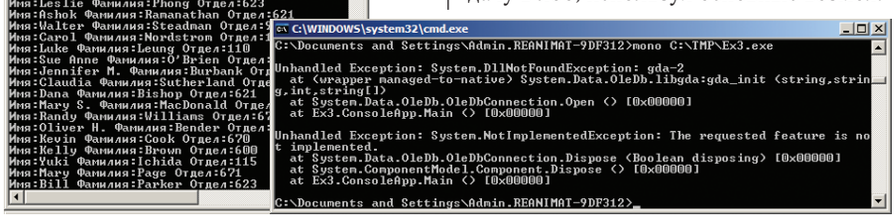
И все это можно делать в Delphi Prism только потому, что реализован полноценный доступ к богатству средств .NET. Аналогичный примененному в нашем примере текст может быть элементом хитрого алгоритма для обработки разнородных данных из различных источников.

Теперь перейдем к классу TextFieldParser, изначально созданному для программистов, работающих на Бейсике. Для доступа к этому классу надо добавить в программу ссылку на Microsoft.VisualBasic.FileIO (Microsoft.VisualBasic.dll).



Листинг 4. Чтение текстового файла и запись его данных в бинарном формате с помощью сериализации

```
…
[Serializable]
TEMPLOYEE = public class
        public
        EMP_NO:SmallInt;
        HIRE_DATE:DateTime;
        JOB_GRADE:SmallInt;
        SALARY:Decimal;
        FIRST_NAME:String;
        LAST_NAME:String;
        PHONE_EXT:String;
        DEPT_NO:String;
        JOB_CODE:String;
        JOB_COUNTRY:String;
        FULL_NAME:String;
end;
implementation
//В этот раз для чтения текстового файла
//используем класс TextFieldParser
//и сериализуем данные – в этом случае
//записываем их на диск в бинарном формате.
class method ConsoleApp.Main;
    var EMP:TEMPLOYEE;
    win1251:=Encoding.
GetEncoding("windows-1251");
    EMPS:=new ArrayList();
begin
  File.Delete('C:\EMPLOYEE.dat');
  using parser:TextFieldParser:=new
                    TextFieldParser('C:\
```



```
EMPLOYEE.txt',win1251) do begin
    parser.SetDelimiters(";");
  while not(parser.EndOfData) do begin
     var fields:array of string:=parser.
ReadFields();
    //Тут можно что-то сделать
//с полями строки
        EMP:=new TEMPLOYEE();
        EMP.EMP_NO:=SmallInt.
Parse(fields[0]);
        EMP.HIRE_DATE:=DateTime.
Parse(fields[4]);
        EMP.JOB_GRADE:=SmallInt.
Parse(fields[7]);
        EMP.SALARY:=Decimal.Parse(fields[9]);
        EMP.FIRST_NAME:=fields[1];
        EMP.LAST_NAME:=fields[2];
        EMP.PHONE_EXT:=fields[3];
        EMP.DEPT_NO:=fields[5];
        EMP.JOB_CODE:=fields[6];
        EMP.JOB_COUNTRY:=fields[8];
        EMP.FULL_NAME:=fields[10];
        EMPS.Add(EMP);
       end;
 end;
   //Сохраняем список объектов на диск
//в бинарном формате
   // – проводим сериализацию объекта
//класса ArrayList
    using fileStream:=new FileStream('C:\
EMPLOYEE.dat',FileMode.Create) do begin
     (new BinaryFormatter()).
Serialize(fileStream,EMPS);
    end;
 System.Console.ReadLine;
end;
end.
```

Пойдем дальше — перезапишем наш файл в какой-нибудь экзотический формат. На самом деле это будет бинарный формат (т.е. не текстовый), и тогда полученный файл по размеру окажется больше, чем исходный текстовый. Но идея в данном случае заключается не в экономии жизненного пространства на громадном диске, а в универсальности подхода к хранению информации. Метод сериализации позволяет выбрать оптимальный вариант между экономией места на жестком диске (для данного рассматриваемого случая), правилами безопасности и спецификой бизнес-логики, а именно особенностями структуры данных. Здесь имеется в виду ориентация на структуру, оптимизированную не для хранения, а для обработки данных. Сериализация — хорошее решение для сохранения данных программы, написанной под .NET, во временном промежутке между ее сессиями. Но это далеко не единственное применение такого подхода. В нашем варианте мы выбрали бинарный формат для сериализации и получили новый файл EMPLOYEE.dat, в котором хранятся те же данные, что и в EMPLOYEE.txt, но уже в недоступном для постороннего глаза виде. Однако мы выбрали формат, удобный для объекта класса ArrayList — «навороченного» массива объектов. Для сериализации необязательно пользоваться сложными классами-контейнерами, можно написать свою структуру.

В результате работы программы наши записи будут в новом файле представлять собой отпечатки объектов класса TEMPLOYEE. А чтобы компилятор позволил нам это проделать, в описании данного класса надо не забыть поставить атрибут Serializable.

Кстати, заметили ли вы, что объекту класса TextFieldParser пришлось явно указывать кодировку файла?

Следующий пример будет достаточно простым. Проводим десериализацию объекта класса ArrayList (т.е. выполняем действие, обратное сериализации), убеждаемся, что она получилась, выводя уже знакомые данные в консоль, и записываем снова все на диск, только уже в формате XML.

Листинг 5. Десериализация бинарного файла и сериализация в формате XML

```
...
class method ConsoleApp.Main;
var EMP:Ex4.TEMPLOYEE;
    EMPS:=new ArrayList(); i:Integer;
begin
  // Читаем бинарный файл –
  // десериализуем его обратно в объект
//класса ArrayList
  using filestream:=new FileStream('C:\
EMPLOYEE.dat',FileMode.Open) do begin

    EMPS:=(new BinaryFormatter()).
Deserialize(filestream) as ArrayList;

  end;

  for i:=0 to EMPS.Count-1 do begin

   EMP:=(EMPS.Item[i] as TEMPLOYEE);
   System.Console.Writeline(

//Выводим в консоль некоторые столбцы
//Сложно привыкнуть, когда IDE за вас
//постоянно расставляет
//в тексте END к месту и не к месту,
//иногда приходится долго
//искать следы этих диверсий!

//Выборочно выводим в консоль значения
столбцов
String.Format('{0}'+Chr(9)+'{1}'+Chr(9)+'{2}'+
Chr(9)+'{3}'+Chr(9)+'{4}',
                EMP.EMP_NO.ToString,
                EMP.DEPT_NO.ToString,
                EMP.HIRE_DATE.
ToShortDateString,
                EMP.FULL_NAME,
                EMP.SALARY)
   );

  end;
   //Сохраняем список объектов на диск
//в формате XML,
   //т.е. опять проводим сериализацию, но
//уже с использованием класса
SoapFormatter
    using fileStream:=new FileStream('C:\
EMPLOYEE.xml',FileMode.Create) do begin

     (new SoapFormatter()).
Serialize(fileStream,EMPS);

    end;

  System.Console.ReadLine;

end;
end.
```

На выходе получили громадный файл (по сравнению с предыдущими), имеющий, однако, открытый формат — важнейшее из преимуществ, которое дает XML.

Итак

В статье мы тактично обошли вопрос, связанный с особенностями работы с бинарными файлами произвольного формата с использованием класса FileStream, не связанного с сериализацией. Также не рассматривалась похожая тема работы с текстовыми файлами, имеющими поля фиксированной длины, но не имеющими разделителей.

Оба этих вопроса лежат глубже рассматриваемой темы, поскольку связаны с другими технологиями платформы .NET, выходящими далеко за рамки данной статьи. ●

— Михаил Перов

Литература

1. Строки форматирования в .NET, www.jenyay.net, www.realcoding.net
2. Keith Rimington. Basic File IO and the DataGridView, www.codeproject.com
3. Nitin Kunte. Get System Info using C# , www.codeproject.com
4. Stephan Depoorter. Handling Fixed-width Flat Files with .NET Custom Attributes, www.codeproject.com
5. Jeff Brand. Converting CSV Data to Objects, www.codeproject.com
6. Oleg Axenow.Работа со строками, www.gotdotnet.ru
7. Savage, Read and Write Structures to Files with .NET, www.codeproject.com
8. Сергей Иванов, Работа с кодировкой DOS, www.realcoding.net
9. Jan Schreuder.Using OleDb to Import Text Files (tab, CSV, custom), www.codeproject.com
10. Jisu74.Read a certain line in a text file, www.codeproject.com
11. Dreamzor, Getting File Info, www.codeproject.com
12. How to copy a String into a struct using C#, www.codeproject.com
13. Arun GG, www.csharphelp.com ,TextReader and TextWriter In C#
14. BLaZiNiX, An INI file handling class using C#, www.codeproject.com
15. C# 2008 и платформа .NET 3.5 для профессионалов.Christian Nagel, Bill Evjen, Jay Glynn, Karli Watson, Morgan Skinner. Диалектика

Смарт-тег для расширения меню пользователя Microsoft Outlook

В данной статье мы рассмотрим, как расширить меню пользователя, появляющееся по нажатию правой кнопкой мыши на имени отправителя или получателя в форме письма. В пункт меню «Дополнительные действия» (Additional Actions) можно добавить действия, написав смарт-тег и зарегистрировав его определенным образом.

Смарт-теги (smart tag, в пер. с англ. — «контекстная метка») выполняют определенные контекстно-зависимые действия при распознавании текстовых фрагментов.

Смарт-теги придуманы для того, чтобы тратить минимум усилий на переключение между приложениями во время работы. Например, можно написать смарт-тег, способный распознавать номера телефонов на основе шаблона и предлагающий занести телефон с именем абонента в CRM-систему. Или смарт-тег, способный распознавать курсы валют на сайте РБК и предлагающий занести их в автоматизированную банковскую систему.

Сценарий работы смарт-тега примерно таков:

- распознавание текстового фрагмента и отображение меню, ассоциированного с данным типом смарт-тега (класс Recognizer);
- выполнение определенных действий (класс Action).

В Интернете имеется масса статей о создании смарт-тегов, расширяющих функциональность офисных продуктов, но лишь немногие из них описывают расширение меню «Дополнительные действия». Буду рада, если мой опыт написания такого смарт-тега на C#.NET окажется полезен читателям.

Для определенности: смарт-тегом будем называть обработчик, реализуемый в виде xml или dll.

Пути решения

Outlook 2007 предоставляет богатые возможности пользовательской настройки меню, но меню «Дополнительные действия» в имеющихся версиях Office расширить стандартными методами, к сожалению, нельзя.

В простейших случаях можно добавить элементы меню с помощью специального xml-файла, как указано в статье [2][1]. Часто этого бывает достаточно, однако сложные случаи, например добавление в название элемента меню имени пользователя, как на рис. 1, придется реализовывать в виде DLL-обработчика.

Реализация

Для создания DLL-обработчика необходима библиотека типов Microsoft Smart Tags 2.0 (MSTag.tbl), которая входит в состав MS Office.

Для начала разработаем обертку (wrapper) этой биб-лиотеки, используя Visual Studio 2005.

- Откроем Visual Studio Command Prompt **(Start • Programs • Visual Studio .NET • Visual Studio .NET Tools • Visual Studio .NET 2005 Command Prompt)**.
- Сгенерируем ключи для подписи сборки (strong name):

```
sn -k SmartTagLib.snk
```

- Перейдем в директорию C:\Program Files\Common Files\Microsoft Shared\Smart Tag и напишем в командной строке примерно следующее:

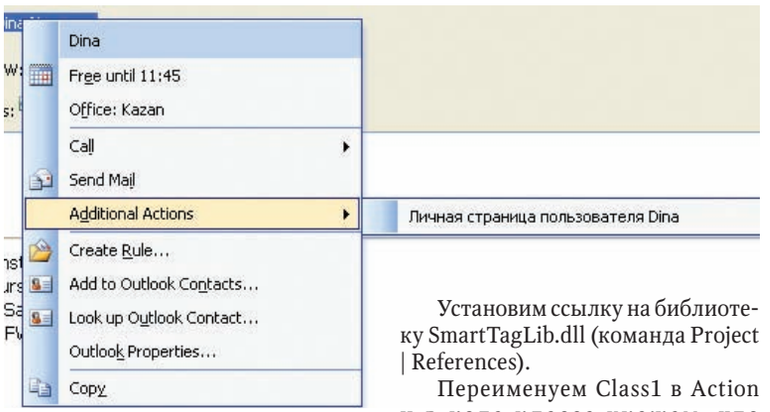
```
tlbimp mstag.tlb /keyfile:c:\
SmartTagLib.snk /out:c:\SmartTagLib.
dll
```

указав вместо «c:\» путь, где должна лежать библиотека SmartTagLib.dll.

Рассмотрим интерфейсы, предоставляемые этой библиотекой.

ISmartTagRecognizer и ISmartTagRecognizer2 отвечают за распознавание текста в документе. При создании смарт-тега для рас-

[1] См. список рекомендованной литературы в конце статьи.



А так будет выглядеть модифицированное меню MS Outlook после добавления смарт-тегов

ширения меню реализовывать этот интерфейс не нужно.

ISmartTagAction и ISmartTagAction2 отвечают за визуализацию пункта меню и действия, которые будут происходить при его выборе. ISmartTagAction2, появившийся в Office 2003, предоставляет методы get_VerbCaptionFromID2 и InvokeVerb2, которые дают возможность менять отображаемое имя смарт-тега в момент инициализации. Эти методы нам помогут, когда мы будем добавлять имя пользователя в элемент меню.

Далее создадим новый проект Class Library и назовем его STPersonaMenu.

Установим ссылку на библиотеку SmartTagLib.dll (команда Project | References).

Переименуем Class1 в Action и в коде класса укажем, что он будет реализовывать интерфейсы ISmartTagAction и ISmartTagAction2.

```
public class Action :
ISmartTagAction, ISmartTagAction2
```

Добавим в начало кода директиву

```
using Microsoft.Office.Interop.
SmartTag;
```

С помощью intelliSense добавим заглушки свойств методов интерфейсов в наш класс.

Обратите внимание на следующие свойства смарт-тега.

В интерфейсе ISmartTagAction:

■ ProgId — идентификатор смарт-тега:

```
public string ProgId
 {
  get
   {
    return "SPAdditionalMenu.
Action";
   }
 }
```

■ Уникальное имя смарт-тега

```
public System.String
      get_SmartTagName
      (System.Int32 SmartTagID)
 {
  return
   "urn:schemas-microsoft-com:
   office:smarttags#PersonName";
 }
```

«urn:schemas-microsoft-com:office:smarttags #PersonName» — тип, включенный в Office для смарт-тега, реализующего дополнительное меню [8][1].

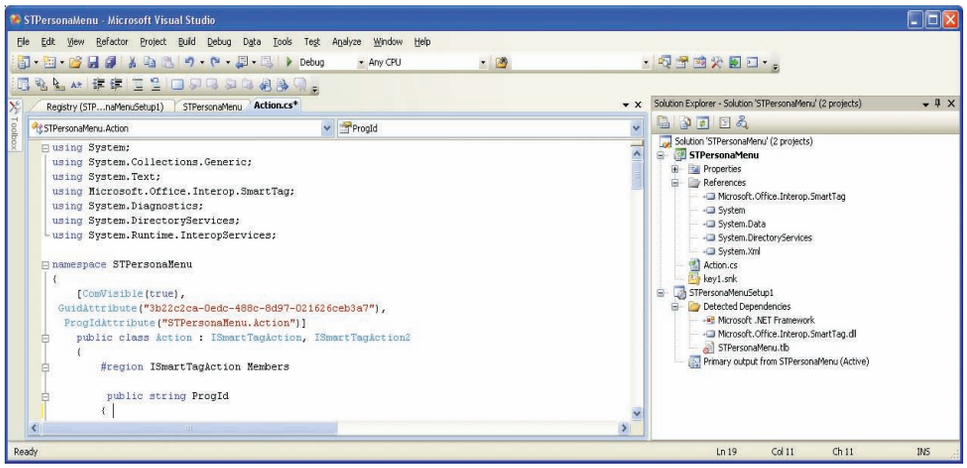
■ VerbCaptionFromID — название пункта меню, которое визуализируется в меню «Дополнительные действия». Если мы определим это свойство, текст, отображаемый в названии пункта меню, будет статическим. Нам же нужно, чтобы он динамически менялся, добавляя в конец имя выбранного пользователя.

Для этого рассмотрим подробнее интерфейс ISmartTagAction2:

■ Из списка параметров, передаваемых в VerbCaptionFromID, нам наиболее интересен Text, который содержит имя пользователя. Добавим его к названию элемента меню.

```
public System.String get_
VerbCaptionFromID2(int VerbID, string
ApplicationName, int LocaleID,
ISmartTagProperties Properties,
string Text, string Xml, object
Target)
{
    return "Личная страница пользо-
вателя" + Text;
}
```

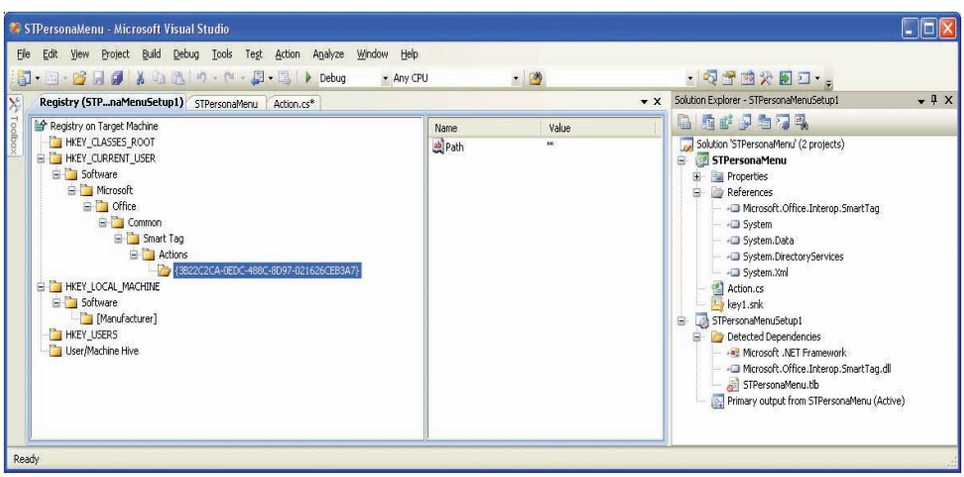
■ IsCaptionDynamic указывает, является ли заголовок элемента меню смарт-тега динамическим. Если да, то при каждом отображении меню вызывается метод SmartTagInitialize. Даже если нам не пригодится этот метод, необходимо установить параметр в true, иначе динамического добавления имени пользователя не произойдет.



Создадим новый проект

```
public bool get_IsCaptionDynamic(int
VerbID, string ApplicationName, int
LocaleID)
{
    return true;
}
```

Добавим информацию в реестр



■ InvokeVerb2 — в этом методе мы определим, что будет происходить при выборе элемента меню. В нашем случае пользователь будет перенаправляться на страницу на корпоративном портале.

```
public void InvokeVerb2(int
VerbID, string ApplicationName,
object Target, ISmartTagProperties
Properties, string Text, string Xml,
int LocaleID)
{
   string url = "http://
myCorporateUrl/personPages";
    System.Diagnostics.Process.Start(
url+ ResolveDisplayNameToADName(Te
xt));
}
```

Не будем описывать здесь все методы, полная реализация смарт-тега приведена на «Мир ПК-диске».

Установка

Рассмотрим случай, когда нужно сделать простенький инсталлятор для установки на несколько рабочих мест.

Подготовим смарт-тег:

1. В свойствах проекта выберем вкладку Build и установим галочку Register for Com interop.

2. Откроем AssemblyInfo.cs, найдем там ключ

```
[assembly: ComVisible(false)]
```

и установим его в true.

3. Изменим класс Action, добавив атрибуты:

```
    [ComVisible(true),
 GuidAttribute("3b22c2ca-0edc-488c-
8d97-021626ceb3a7"),
  ProgIdAttribute("STPersonaMenu.
Action")]
    public class Action :
ISmartTagAction, ISmartTagAction2
```

Понятно, что идентификатор (GUID) должен быть уникальным.

4. В свойствах проекта выберем вкладку Singing и установим галочку Sing the assembly. В появившемся выпадающем списке выберем New и создадим ключ для подписи.

5. В меню Build выберем Build solution, чтобы создать dll. В дирек-

НОВОСТИ

FSC нарушает законы

Маленькие ноутбуки обычно неповоротливы в играх, а большие — в жизни. Компания Fujitsu Siemens Computers постаралась не спеша решить эту проблему: в середине прошлого года анонсировала технологию GraphicBoosters, а в феврале в России начнутся продажи первого продукта, поддерживающего ее. Комплект из компактного ноутбука Amilo Sa 3650 и внешней графической подсистемы Amilo GraphicBoosters позволяет убить двух зайцев. С одной стороны, пользователь получает компактный и легкий ноутбук, со значительным временем автономной работы, с другой — мощную систему для игр и графических приложений, достаточно только подключить внешний видеоускоритель.

GraphicBoosters представляет собой небольшую пластмассовую коробочку размерами 180x130x34 мм и массой 500 г, внутри которой находится мощная графическая карта ATI Mobility Radeon HD 3870 с 512 Мбайт видеопамяти GDDR3. Помимо специального разъема для подключения к ноутбуку GraphicBoosters оснащен разъемами DVI-I с поддержкой HDCP и HDMI (HDCP и S/PDIF). Также устройство располагает двумя разъемами USB 2.0 для подключения различной периферии.

Ноутбук Amilo Sa 3650 имеет экран диагональю 13,3 дюйма, массу менее 2,5 кг. Он построен на процессоре AMD Turion X2 Ultra и оснащен 4 Гбайт ОЗУ, жестким диском, объемом 320 Гбайт, видеокартой ATI Radeon HD 3200, DVD-приводом SuperMulti и беспроводными адаптерами Wi-Fi и Bluetooth.

P. B.

тории bin\Debug должно появиться три файла: dll, pdb и tlb.

Создадим установщик:

1. Сделаем новый проект Setup and Deployment и назовем его STPersonaMenuSetup.

2. Добавим в него нашу библиотеку (**STPersonaMenuSetup project • Add • Project Output**. В появившемся окне Add Project output Group выберем Primary Output проекта STPersonaMenu). Папка Detected dependencies будет содержать несколько файлов, как указано на рис. 2.

Файлы STPersonaMenu.tlb и MSTag.TLB можно исключить из проекта. Для Primary output from STPersonaMenu и SmartTagLib.dll необходимо указать, что они будут устанавливаться в Global Assembly Cache. Для этого установите в свойствах файла параметр Folder в Global Assembly Cache Folder (возможно, по умолчанию нельзя будет выбрать папку GAC Folder, тогда ее нужно сначала добавить из меню View • File system проекта установщика).

3. Вынесем в реестр информацию о смарт-теге. Для этого откроем меню **View • Registry** проекта и добавим ключи в ветку HKEY_CURRENT_USER, чтобы получилось, как на рис. 3. GUID должен совпадать с указанным в классе Action.

Добавьте строковый или любой другой параметр, чтобы последний ключ был не пустым, иначе ветка не создастся.

4. Компилируем проект и пробуем запустить.

Установщик при запуске добавит необходимые ключи в реестр и файлы SmartTag.dll и STPersonaMenu в GAC, и в MS Outlook появится новый пункт меню «Личная страница пользователя %Username%», при выборе которого будет открываться ссылка http://myCorporateUrl/personPages/%Username%. ●

Рассмотренный пример легко адаптировать для создания смартегов, реализующих любые другие расширения меню «Дополнительные действия».

Дополнительные материалы на «Мир ПК-диске».

— Дина Насырова — разработчик компании Auriga, Inc.

Литература

1. Adding custom menu items to Microsoft Office Communicator 2007 menus http://imwire.eventure.biz/imwire/articles/22.aspx
2. Additional Actions when right-clicking a From or To address.http://www.crmreports.com/index.php/additional-actions-when-right-clicking-a-from-or-to-address.html
3. http://msdn.microsoft.com/en-us/library/aa195565.aspx
4. http://groups.google.co.uk/group/microsoft.public.office.developer.smarttags/browse_thread/thread/4c2c6c177133759f/3e7ca057c391de7e?lnk=st&q=Person+Name+Smart+Tag+Outlook&rnum=6&hl=en#3e7ca057c391de7e
5. ISmartTagAction2 Interface [Office 2003 SDK Documentation] http://msdn.microsoft.com/en-us/library/aa206976(office.11).aspx
6. Smart Tag SDK http://msdn.microsoft.com/en-us/library/bb190881(office.11).aspx
7. Что нового в смарт-тегах Office 2003 http://www.gotdotnet.ru/LearnDotNet/XMLWebServices/29515.aspx
8. Smart Tags and the Persona Menu [Office 2003 SDK Documentation] http://msdn.microsoft.com/en-us/library/aa195475.aspx
9. Register the Visual C# Smart Tag DLL [Office 2003 SDK Documentation] http://msdn.microsoft.com/en-us/library/aa168710(office.11).aspx
10. http://support.microsoft.com/?kbid=306422
11. Build and Deploy a .NET COM http://www.simple-talk.com/dotnet/visual-studio/build-and-deploy-a-.net-com-assembly/
12. How to make a Smart Tag using C# http://www.codeproject.com/KB/cs/smarttag.aspx