

Defacto – специализированное средство аудита программного обеспечения

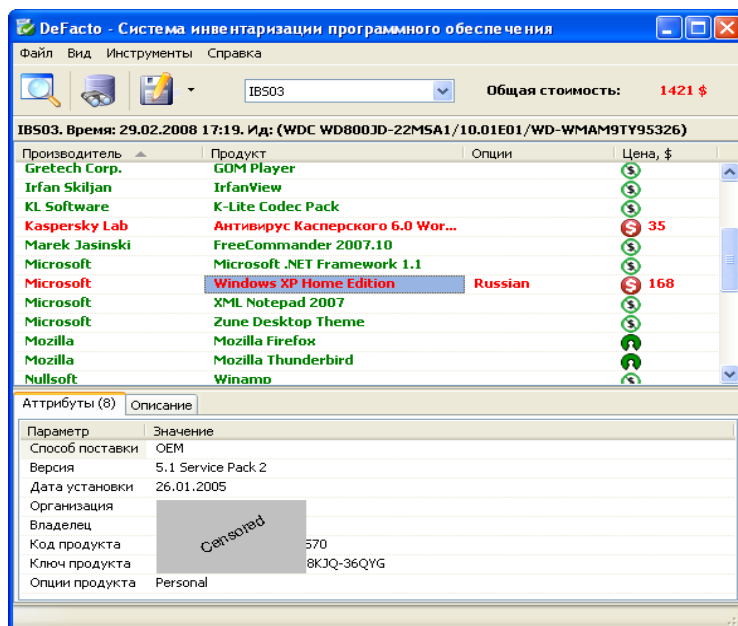
Коршунов Владимир Геннадьевич, генеральный директор ООО «Инфобис»

Автоматизированный аудит программного обеспечения

Под аудитом программного обеспечения подразумевается процесс инвентаризации программ, фактически установленных на компьютерах организации, и сопоставления с данными о легально приобретенных нематериальных активах. На основании данных аудита предпринимаются соответствующие меры: закупка недостающих лицензий или деинсталляция нелегального программного обеспечения.

В данной статье мы рассмотрим именно первую фазу процесса аудита, которая легко поддается автоматизации. Требуется получить список программного обеспечения, установленного на компьютере под управлением ОС Windows, включающий в себя название программного продукта и его производителя («вендора»). Какие формальные методы для этого допустимы?

Первый и самый очевидный способ - это извлечение и анализ заголовков всех файлов, находящихся на жестком диске. Данный способ возможен, но занимает слишком длительное время и не вполне подходит для экспресс-аудита. Тем не менее, именно этот способ используется большинством систем управления активами (asset management software), имеющими собственные базы сигнатур. Разновидностью этого метода является анализ системных журналов, фиксирующих исполняемые файлы, которые запускались на данном компьютере.



Второй способ - это анализ областей, предназначенных для запуска программ пользователем. Такими областями являются меню «Пуск», ярлыки рабочего стола и стандартные каталоги: «Program Files», «Мои документы» и др. Данным способом легко воспользоваться вручную, а для автоматического анализа он недостаточно надежен из-за вероятности произвольного именования файлов и каталогов, а также различного написания названий каталогов на различных языках.

Третий способ - анализ реестра. Большинство приложений сохраняют в реестре базовые сведения о себе (версия, путь установки и др.), а также данные, сформированные в процессе работы (текущие настройки). Также в реестр попадает множество сведений операционной системы, в том числе и список программ, поддерживающих автоматическое удаление. Вручную анализировать реестр несложно, хотя операция это достаточно утомительная, а для автоматического анализа реестр является наиболее подходящим инструментом, поскольку в реестре обычно содержится исчерпывающая информация об установленных приложениях.

Понятно, что идеального способа инвентаризации не существует, но посмотрим на это с практической точки зрения. Будем ставить целью проведение оперативного анализа и идентификации наиболее часто встречающегося программного обеспечения. Причем под идентификацией подразумевается определение типа лицензии на программу (бесплатная, пробная, коммерческая), точного наименования продукта (SKU) и его стоимости.

Решать данную задачу можно введением базы знаний о записях в реестре. Например, Borland Delphi 5.0 создает следующую запись в реестре: HKLM\SOFTWARE\Borland\Delphi\5.0. В ключе Version содержатся значения STD, PRO или CSS, что позволяет точно идентифицировать редакцию продукта (Standard, Professional, Enterprise), а соответственно и его стоимость. В той же ветке содержится информация о покупателе и серийном номере продукта. Аналогичная информация существует и у большинства других производителей.

Дополнительно к методу поиска продуктов при помощи базы знаний, можно воспользоваться более универсальными способами. Подавляющее большинство приложений при установке добавляют запись в ветку реестра HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall, которая используется для построения списка «Установка и удаление программ». Большинство программ также создают записи в ветке HKLM\Software. Совмещение всех этих источников дает наилучший результат, но вручную подобный анализ произвести затруднительно, поэтому рассмотрим практическую реализацию вышеизложенных утверждений.

Существует множество программ для сбора информации об установленном программном обеспечении. Большая часть из них либо не предоставляют требуемой информации и выводят множество ненужной (класс программ для сбора информации об оборудовании), либо довольно громоздки и требуют предварительной настройки (программы для управления активами).

Описание программы «Defacto»

Разработанное нами программное обеспечение «Defacto» (<http://www.defacto-com.ru>) изначально предназначено для проведения экспресс-аудита и, в связи с этим, обладает существенными преимуществами: упрощенный интерфейс, изначально заполненная база знаний, высокая скорость сканирования, возможность работы с переносного накопителя.

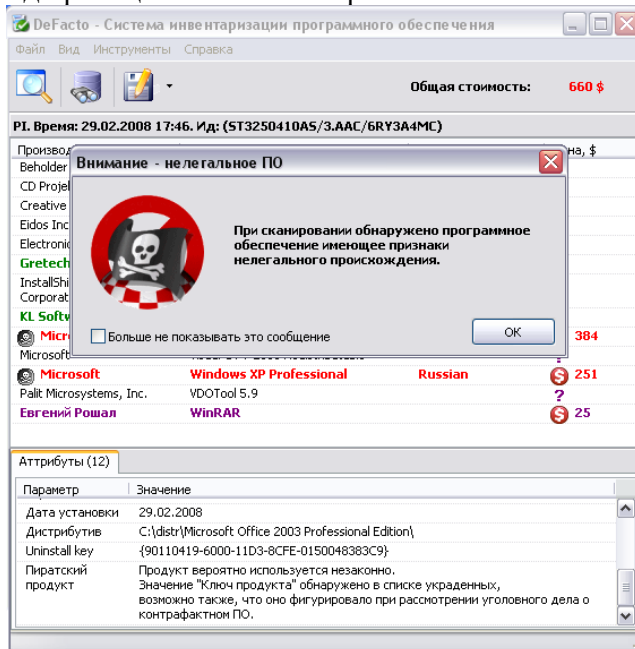
Результаты представляются в виде таблицы, в которую сведены сведения об авторе, названии программы, ее рыночной стоимости, статусе (коммерческая, условно-бесплатная, бесплатная). Бесплатные программы отображаются зеленым цветом, платные — красным, пробные (shareware) — фиолетовым. Если база знаний содержит информацию о цене, то она также будет выведена в соответствующей колонке. Итог по этой колонке означает общую стоимость установленного программного обеспечения.

Для программ определяется и выводится в закладке «Атрибуты» дополнительная информация включающая: дату и каталог установки, путь к дистрибутиву, версию/сборку. Может быть определен код продукта, серийный номер, ключ продукта, способ поставки (FPP, OEM и т.д.), а также имя зарегистрированного владельца.

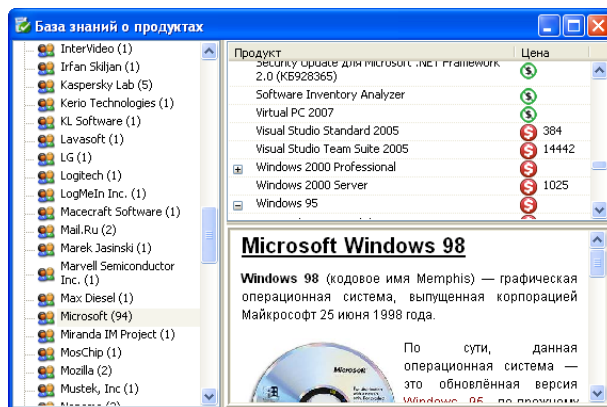
Для повышения информативности системные программы, драйвера и обновления не отображаются в списке, но, при необходимости, из меню «Вид» можно включить их показ. Для той же цели повышения информативности, предусмотрена возможность скрыть бесплатные программы и оставить только программы, имеющие коммерческую или неопределенную программой «Defacto» лицензию.

Уникальной возможностью «Defacto» является определение признаков нелегального использования продукта. Такими признаками могут являться: пиратский или фигурировавший при рассмотрении дела о контрафактном программном обеспечении серийный номер, наличие следов «взлома» систем защиты коммерческих продуктов и другие признаки. Продукт, имеющий признаки нелегального использования, помечается в списке специальным значком, а после завершения процесса сканирования выдается привлекающее внимание сообщение.

Еще одним преимуществом программы «Defacto» является то, что сканирование может быть проведено как для локальной системы (поддерживаются все ОС семейства Windows начиная с Windows 95 и заканчивая Windows Vista), так и для системы находящейся в неактивном (незагруженном) состоянии. Сканирование неактивной системы производится выбором каталога ОС Windows на любом из доступных носителей. Эта возможность позволяет проводить инвентаризацию установленного программного обеспечения на жестких дисках, ранее установленных в других компьютерах. При этом операционная система с жесткого диска не запускается, и даты модификации системных файлов остаются неизменными.



Собранные данные могут быть сохранены в файл, для последующего детального анализа собранной информации. Также реализована возможность экспорта в текстовый файл и файл Excel (при этом наличие самой программы Microsoft Excel не требуется). Данные могут быть объединены для получения сводного отчета, в котором отображается информация по суммарному количеству установленных копий каждого из продуктов и на каких компьютерах установлен данный продукт.



«Defacto» включает в себя каталог продуктов с кратким описанием программы, списком ее версий и модификаций, информацией о стоимости. В базе знаний также содержатся данные о производителях, ключах реестра для поиска продуктов, отпечатках пиратских серийных номеров и другая информация. Конечно, база не является всеобъемлющей и содержит только ту информацию, которую в нее добавили разработчики, но она регулярно пополняется и может быть автоматически обновлена через сеть Интернет.

«Defacto» занимает мало места на диске, не требует установки и может работать с переносного диска – флэш-накопителя, причем сам накопитель можно защитить от записи для противодействия компьютерным вирусам. Все это позволяет использовать «Defacto» в качестве

инструмента экспресс-аудита в том числе и на компьютерах, имеющих сомнительное происхождение.

Применение «Defacto» для защиты авторских прав

В настоящее время программа «Defacto» применяется экспертами компьютерной и компьютерно-технической экспертизы при производстве экспертиз по уголовным делам по ч.2 и ч. 3 ст. 146 УК РФ. С помощью программы эффективно выявляется и описывается установленное на исследуемом компьютере программное обеспечение, определяются его регистрационные данные и обстоятельства установки (дата, расположение дистрибутива на носителях информации).

Иногда в качестве недостатка программы отмечается невозможность детектирования дистрибутивов программ, размещенных на исследуемом носителе информации. В соответствии с действующим законодательством дистрибутив программы также является экземпляром программы, как и проинсталлированная копия. Но действительно ли отсутствие детектирования дистрибутивов является недостатком с точки зрения следствия? Для того чтобы обвинить кого-либо в совершении преступления, предусмотренного ч.2 и ч.3 ст. 146 УК РФ, необходимо доказать, что у человека был умысел, например, в виде извлечения прибыли из незаконного использования чужих объектов авторского права. Одно лишь наличие на диске дистрибутива не указывает на то, что им хоть однажды воспользовались, в то время как проинсталлированная программа – это верный признак того, что осуществлялось копирование файлов программы (получение нового экземпляра программного обеспечения из его дистрибутива). Более того, не всегда возможно доказать, что владелец или пользователь компьютера, на носителях которого обнаружен данный дистрибутив, знал о существовании данного файла на диске. Поэтому детектирование именно установленных, запускавшихся и доступных из интерфейса ОС программ дает перечень программных продуктов, о существовании которых пользователь не мог не знать.

Также программа «Defacto» используется оперативными сотрудниками МВД для приблизительной оценки стоимости программных продуктов при проведении проверок хозяйственной деятельности организаций. Хотя оценка именно приблизительная и требует дальнейшего уточнения экспертами, она дает представление о масштабах нарушений авторских и смежных прав сотрудниками организации и позволяет принять решение об обоснованности изъятия средств вычислительной техники.