



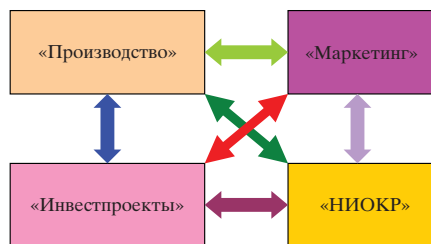
ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ В ПРОМЫШЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Л. С. Раткин,

действительный член Международной академии информатизации, к. т. н.

Современное промышленное производство невозможно представить без информационных систем (ИС), при этом на рынке программных продуктов наблюдается стабильный рост количества ИС, охватывающих несколько стадий жизненного цикла (ЖЦ) продукции. Концепция непрерывной информационной поддержки ЖЦ продукции (Continuous Acquisition and Life-cycle Support — CALS) реализуется в различных системах управления ЖЦ изделия (Product Lifecycle Management — PLM) [1].

Каковы основные стадии ЖЦ продукции? Прежде всего, следует выделить маркетинг, способствующий выявлению ее конкурентных преимуществ по сравнению с аналогами и разработке с учетом полученной информации новых типов изделий. Концепция продукции находит отражение в проектировании изделия, планировании и разработке соответствующих процессов. Подготовка производства предполагает также обеспечение трудовыми и сырьевыми ресурсами, закупку комплектующих и материалов. Выпуск изделий сопровождается предоставлением услуг по упаковке, складированию и реализации через сервисную сеть, монтажу, технической поддержке, гарантийному и постгарантийному обслуживанию. Утилизация завершает ЖЦ продукции и предполагает новый виток ЖЦ с учетом полученных рекомендаций, рекламаций, оптимизации технических решений и технологических процессов для изделий данной товарной группы, занимающих на рынке определенную ценовую нишу, обладающих рядом потребительских свойств и имеющих фиксирован-



ный и прогнозируемый к расширению сегмент сбыта.

Рассмотрим корпоративную ИС (КИС), включающую в себя ряд информационных систем: «Маркетинг», «НИОКР», «Инвестпроекты» и «Производство». В каждой из систем содержится данные о конкретной стадии ЖЦ продукции, при этом возникает задача соблюдения целостности передаваемых сведений и обеспечения конфиденциальности информации. Поскольку каждая ИС может быть установлена на отдельном предприятии, задача их объединения в КИС решается в рамках формирования вертикальной интегрированной структуры — процесса, достаточно часто встречающегося в последнее время в нефтяной, оборонной и других отраслях. Процедура консолидации данных, формирования корпоративной отчетности в условиях разрозненности информационных источников накладывает определенные ограничения на параметры функционирования КИС.

Прежде всего, к числу ограничительных относится временной фактор — различная пропускная способность телекоммуникационных каналов предполагает снижение скорости обработки информационных массивов при сложном перекрестном запросе к различным базам данных разных ИС. Кроме того, любое не-

рациональное распределение информации предполагает дополнительные затраты на ее актуализацию, в том числе физические (лишний расход памяти), финансовые (избыточная оплата) и временные (простой системы). Наконец, устойчивость КИС к сбоям, вирусным и хакерским атакам должна быть обеспечена благодаря высокой степени защиты с применением современных технологий информационной безопасности, причем не только криптографических, но и стеганографических.

Пусть i — номер изделия ($i = 1 \dots N$), по которому каждая единица продукции однозначно идентифицируется в разных промышленных ИС. Тогда $a_i(t)$ — суммарный объем информации об изделии, хранящейся в КИС. Он складывается из открытой и закрытой частей — $b_i(t)$ и $c_i(t)$. Соответственно: $a_i(t) = b_i(t) + c_i(t)$. Заметим, что $a_i(t)$, $b_i(t)$, $c_i(t)$ — монотонно растущие функции (данные об изделии с течением времени t накапливаются). Для защиты закрытых данных необходимо обеспечить непрерывный приток в КИС стеганографических контейнеров, позволяющих на любой фиксированный момент времени t сохранять закрытую информацию в объеме $c(t) = c_1(t) + c_2(t) + c_3(t) + \dots + c_N(t)$. Достигается это комбинацией следующих способов.

Во-первых, в распоряжении администратора КИС должны находиться стегоконтейнеры, причем не только пустые, но и частично заполненные. С помощью средств стегоанализа КИС производится расчет предельно допустимого объема закрытой информации, которая может быть помещена в каждый из

контейнеров. Поскольку размеры (и, соответственно, емкость) каждого из контейнеров зависят от объема данных, хранимых в файлах-контейнерах обычным способом (то есть без применения стегосредств), объем доступного адресного пространства стегоконтейнеров должен быть не ниже (а чаще — превосходить) $c(t)$.

Во-вторых, для повышения устойчивости к взлому возможно снижение размера стегокванта (порции скрываемой информации) и применение различных механизмов (например, перекрестных ссылок), многократно усложняющих процедуру распознавания скрытого сообщения (или его фрагмента), применяемую в современных стеганографических системах. Пересчет размера каждого стегокванта в КИС сопровождается перерасчетом суммарного адресного пространства для закрытых данных. Таким образом, если в КИС присутствует избыточное количество стегоконтейнеров, администратору может быть предложено в автоматическом режиме уменьшить размер стегокванта и перераспределить суммарный объем закрытых данных по большему количеству контейнеров. Выполнение этой операции не займет много времени — действие будет выполняться параллельно с текущими заданиями по обработке сведений в КИС, и по истечении временного интервала T_0 перераспределение информации будет завершено.

В-третьих, применяемый в КИС механизм планирования и распределения ресурсов может использоваться для решения внутрисистемных задач. Например, по каждому изделию производится регулярное сохранение данных об объеме закрытой информации (в том числе о количестве характеристик, зарубежных аналогах, результатах испытаний). На основании подробной статистики осуществляется планирование потребности в стегоконтейнерах на ближайшую перспективу. Заметим, что с течением времени контейнеры могут освобождаться вследствие архивирования (то

есть сжатия и/или перемещения на удаленные носители) части редко используемых сведений, например о снятых с производства типах продукции.

Для распределения закрытых данных возможно использование стегорепозитория, в котором хранится информация о местонахождении каждого стегокванта в любом из контейнеров. В отличие от обычных репозиторий, хранящих и обрабатывающих данные и метаданные в разных версиях с отображением эволюции их структур [2], стегорепозитории используют в работе механизмы скрытого хранения и обработки информации. Так, в дополнение к адресу блока закрытых данных предоставляются сведения об использованных стеганографических методах, количестве и типах стегоконтейнеров, их местонахождении и последовательности чтения. Поскольку стегорепозиторий является ядром системы защиты, для обеспечения его безопасной (скрытой) эксплуатации также предполагается применение соответствующих методов. Таким образом, построенный репозиторий имеет приставку стего- не только за счет применения методов компьютерной стеганографии (КС) для сокрытия хранимых и обрабатываемых данных и метаданных различных версий с отображением эволюции структур, но и благодаря сокрытию самого репозитория как объекта благодаря комбинированию криптографических и КС-методов.

В качестве контейнеров для стегорепозитория могут использоваться:

- графические файлы (рисунки, схемы, чертежи, эмблемы, эскизы, плакаты, фотографии и другие типы иллюстраций);
- видеофайлы (видеозаписи фрагментов полевых испытаний новых образцов военной техники и вооружения);
- речевые файлы (в частности, с записью переговоров о подписании договоров о намерении, контрактов, актов приемки-передачи) и т. д.

ВЫВОДЫ

Применение при проектировании промышленных КИС стегорепозиторий с помощью современных КС-инструментов повышает уровень защиты данных и снижает риск взлома систем, а также затраты на обеспечение информационной безопасности. Высокая наукоемкость КС-разработок предполагает первоочередное использование стегосистем в отраслях, имеющих инвестиционную привлекательность для отечественного и зарубежного бизнеса.

Среди отраслей российской промышленности, обладающих высоким инвестиционным потенциалом, можно выделить топливно-энергетический комплекс, а также транспорт и строительство. Так, вопросы управления ЖЦ продукции были затронуты на Всероссийском энергетическом форуме «ТЭК России в XXI веке», проходившем в Москве с 3 по 7 апреля 2006 года.

Применение КС в криминалистике требует принципиально иных подходов, которым будет посвящена следующая публикация.

ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА

1. Информационное обеспечение, поддержка и сопровождение жизненного цикла изделия / Под ред. В.В. Бакаева. — М.: Машиностроение-1, 2005.
2. Коголовский М.Р. Энциклопедия технологии баз данных. — М.: Финансы и статистика, 2005.