

УДК 658.512.011.56

Возможности использования метода результативного искажения при создании сложных технических систем в высокотехнологичных отраслях промышленности

С.Б.Коршиков, М.Н.Терентьев, М.Н.Мусолов

Аннотация

В статье анализируется возможность использования в реальной сфере экономики метода результативного искажения, обеспечивающего повышение производительности шифрования и предотвращение снижения криптостойкости при защите информации геометрических моделей изделий от несанкционированного доступа. Сделан вывод о возможности применения метода в авиационной промышленности.

Ключевые слова: геометрическая модель, распределенное предприятие, метод результативного искажения, условия применимости, отрасль промышленности

На современном этапе развития промышленности основным типом предприятия фактически стало «распределенное предприятие». Всеобъемлющее проникновение такого типа предприятия тем более обосновано в наукоемких отраслях промышленности, в которых для достижения успеха не достаточно усилий одного отдельно взятого предприятия. Конкурентная борьба и необходимость повышения экономической эффективности производства требуют тесной кооперации большого числа партнеров, являющихся признанными мировыми лидерами в своих отраслях. Одним из ярких примеров подобной консолидации усилий большого числа мировых компаний, направленной на создание высококачественной продукции, является международная кооперация в разработке и производстве семейства среднемагистральных гражданских самолетов Sukhoi SuperJet.

Жизненный цикл (ЖЦ) многих изделий авиационной и ракетно-космической промышленности состоит из многих стадий (рис. 1), на каждой из которых партнеры взаимодействуют друг с другом при помощи электронных документов. Во многих случаях такое взаимодействие происходит посредством открытых каналов передачи данных. В связи с этим актуальной является задача защиты как информации геометрических моделей, так и

других сопутствующих данных. Для повышения производительности шифрования и исключения снижения криптостойкости был предложен метод результативного искажения [1], суть которого кратко изложена ниже.

Вместо шифрования модели в целом метод результативного искажения (МРИ) предполагает искажение основных параметров геометрической модели и шифрование истинных значений измененных параметров. Искаженная модель и зашифрованный набор параметров могут быть переданы по открытым каналам связи. Получатель должен расшифровать истинные значения параметров и восстановить исходную модель. МРИ решает вопросы классификации моделей (например, не имеет смысла искажение стандартных деталей) и параметров (не все параметры в одинаковой степени влияют на изменение модели), обратимости искажения (не любое изменение модели является обратимым).

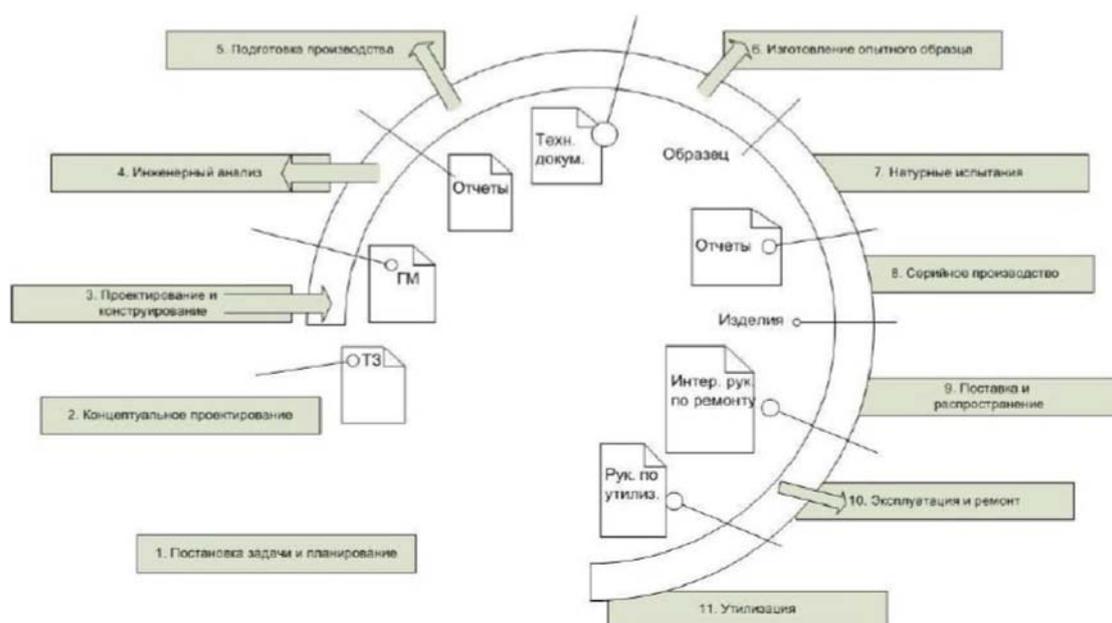


Рис. 1. Жизненный цикл изделия.

В этой связи встает вопрос о необходимости исследования применимости предложенной схемы защиты информации, основанной на МРИ, в различных отраслях промышленности.

Первым условием приемности (рис. 2) является распределенный характер предприятия. В случае, когда все работы сконцентрированы на одной небольшой территории, есть возможность изолировать группу компьютеров, используемых для работы над изделием, от внешнего мира, и тем самым избежать утечки конфиденциальной информации. При использовании распределенного предприятия, характерного для тесной кооперации многих предприятий авиационной промышленности, такой возможности нет.

Вторым условием является готовность распределенного предприятия к работе по предложенной схеме. Данное условие подразумевает не только применение современных систем CAD и PDM, обеспечивающих создание параметризованных геометрических моделей [2], но и определенный уровень культуры обращения персонала с данными геометрических документов.



Метод результативного искажения ПРИМЕНИМ

Рис. 2. Условия применимости метода результативного искажения.

Третье условие применимости заключается в том, что информация, которой обмениваются партнеры, объединенные в распределенное предприятие, составляет коммерческую тайну, и нуждается в защите.

С учетом сформулированных условий можно сделать вывод о том, что предложенная схема защиты информации применима в следующих отраслях реального сектора экономики:

- авиационная промышленность гражданского назначения,
- гражданское судостроение,
- автомобилестроение,
- станкостроение,
- производство бытовой техники и товаров народного потребления. Поясним

сделанный вывод. Каждая из названных отраслей реального сектора экономики характеризуется необходимостью глубокой кооперации взаимодействующих компаний на всех этапах жизненного цикла изделия, таким образом в производстве конечного изделия участвует распределенное предприятие. При этом во многих компаниях используются современные системы CAD и PDM, обеспечивающие необходимый уровень работы с документами геометрических моделей [3]. Начиная с проработок перспективного изделия в дизайнерском бюро, между партнерами происходит интенсивный обмен материалами, составляющими коммерческую тайну, в том числе, посредством публичных сетей. Немалая часть этих материалов представляет собой геометрические модели деталей и сборочных узлов [4]. Например, предложенная схема защиты информации применима в рамках уже упомянутой кооперации при разработке самолета Sukhoi SuperJet.

Использование предложенной схемы защиты конструкторской информации на основе МРИ позволяет снизить расходы на защиту информации при взаимодействии партнеров по разработке и производству изделий за счет 1) возможности использования открытых каналов связи, 2) многократного снижения подлежащего шифрованию объема данных, 3) скрытия от потенциальных злоумышленников самого факта использования средств защиты информации и, как следствие, 4) повышения криптостойкости защищенных данных.

Применение предложенной схемы эффективно на следующих этапах жизненного цикла изделия:

- на этапе разработки обмен данными между группами конструкторов совместно участвующих в разработке компаний, позволяющий максимально использовать накопленный каждым из партнеров опыт,
- на этапе подготовки производства двусторонний обмен данными между конструкторами и серийными заводами, приводящий к повышению качества и снижению себестоимости продукции,
- на этапе опытного и серийного производства обмен данными между взаимодействующими серийными заводами, поставщиками компонентов и т. д.,
- на этапе эксплуатации обмен данными между эксплуатантами, сервисными организациями, серийными заводами и разработчиками с целью решения проблем, вызванных эксплуатацией изделия у клиента, повышения качества и безопасности изделий путем своевременной модификации, сопряженной с выпуском извещений об изменениях и т. п. вспомогательной документации. В дополнение к сформулированным ранее условиям применимости необходимо

отдельно отметить случаи, в которых использование предложенной схемы защиты информации невозможно или неэффективно.

Во-первых, к таким случаям относится разработка и производство вооружений и спецтехники. Для предотвращения утечек информации геометрических моделей таких изделий должны применяться иные средства защиты.

Во-вторых, внедрение предложенной схемы защиты информации геометрических моделей не даст необходимого эффекта в случае, если бизнес-процесс разработки и производства изделий хотя бы у одного взаимодействующего партнера построен на основе бумажных чертежей, а не электронных моделей. Другим препятствием аналогичного типа является организация работ на предприятии по типу «стихийной» автоматизации.

Подводя итог вышесказанному, можно сделать вывод о том, что предложенная схема защиты информации подходит для многих предприятий авиационной и ракетно-космической промышленности, участвующих в кооперативной работе над изделием и испытывающих потребность в защите коммерческой тайны. Более того, готовность предприятия работать по предложенной схеме может положительно повлиять на получение данным предприятием подряда на выполнение работ.

Работа выполнена в рамках НИР (ГК П1959) по ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009 – 2013 годы.

Библиографический список

1. Коршиков С.Б., Падалко С.Н. Метод результативного искажения параметров двухкомпонентной геометрической модели для обеспечения безопасности ее передачи по открытым каналам // Вестник МАИ. — М.: Изд-во МАИ, 2008 г. — № 1: Т. 15. — с. 126-135.
2. Борисов С.А., Смолянинов В.В., Терентьев М.Н. Способы создания параметризованной геометрической модели. // Материалы межд. конф. «Восток-Запад. Информационные технологии в проектировании». — М., 1995.
3. Давыдов Ю.В. Опыт применения информационных технологий НИЦ АСК в аэрокосмической промышленности // Вестник машиностроения. — 1998. — №5. — с. 34-40.
4. Мендзевровский И.Б., Гарусов В.Н., Светцов Н.В. К вопросу управления жизненным циклом изделия в виртуальных компаниях // Информационные технологии в наукоемком машиностроении. — К.: Техника, 2001. — с. 525-569.

Сведения об авторах

Сергей Борисович Коршиков, старший преподаватель Московского авиационного института (национального исследовательского университета), к.т.н. МАИ, Волоколамское ш., д. 4, Москва, А-80, ГСП-3, 125993, тел. (499) 158-45-30, e-mail: s.b.korshikov@gmail.com

Максим Николаевич Терентьев, старший преподаватель Московского авиационного института (национального исследовательского университета), к.т.н. МАИ, Волоколамское ш., д. 4, Москва, А-80, ГСП-3, 125993, тел. (499) 158-45-30, e-mail: m-te@yandex.ru

Максим Николаевич Мусолов, аспирант Московского авиационного института (национального исследовательского университета). МАИ, Волоколамское ш., д. 4, Москва, А-80, ГСП-3, 125993, тел. (499) 158-45-30, e-mail: mmusolov@gmail.com