Мелихов А.А.

Обеспечение непрерывной разработки программных продуктов, сертифицируемых по требованиям безопасности

Аннотация: В настоящей работе рассмотрена проблематика сертификации коммерческих программных продуктов по требованиям безопасности, предложена модель гибридного производственного цикла, обеспечивающего процесс непрерывной поставки обновлений.

Ключевые слова: гибкие методологии разработки, сертификация программных продуктов, импортозамещение, безопасная разработка, CI/CD, оптимизация производственных процессов

Сертификация программного обеспечения представляет собой независимую комплексную экспертизу на предмет соответствия требованиям нормативной документации по информационной безопасности. В рамках сертификации проверяются такие свойства программного продукта, как отсутствие недекларированных возможностей и известных уязвимостей в компонентах программного обеспечения, применение исключительно надежных криптографических средств и т.д. В этом процессе сертификационная лаборатория является внешней незаинтересованной стороной и функционирует в отличном от отраслевых стандартов разработки программного обеспечения режиме.

В случае, если производство сертифицируемых продуктов является для организации основным видом деятельности, данное обстоятельство не представляет собой серьезную проблему, т.к. весь процесс производства согласован с работой лаборатории. Однако если сертификация производится для определенной конфигурации некоторого базового продукта, создается эффект «бутылочного горлышка», когда производство стабильно выпускает обновления, при этом цикл подготовки к сертификации занимает больше времени, чем цикл подготовки релиза базовой версии. Как следствие, за время одного цикла сертификации продукт устаревает как минимум на один релиз относительно базового, а если

требуется выпуск продуктов по разным группам требований, то трудозатраты по подготовке возрастают кратно.

В рамках настоящей публикации рассмотрен подход к организации производственного цикла сертифицируемого программного обеспечения, в настоящий момент проходящий апробацию в кампании ООО «Новые Облачные Технологии». Целью подхода является снижение трудозатрат на производство сертифицируемого продукта при поддержании темпов его обновления.

Проблематика

Гибкие методологии разработки программного обеспечения получили широкое распространение в конце XX – начале XXI века как замена традиционных «водопадных» методов. Вне зависимости от конкретной реализации (RAD, SCRUM, экстремальное программирование) в их основе лежат единые принципы организации производственного процесса, такие как планирование короткими интервалами (спринтами), глубокая декомпозиция задач, акцент на самоорганизацию производственного коллектива [1]. Отдельная роль определена и для средств автоматизированной обработки информации: снижение накладных затрат на передачу контекста решаемых проблем (программного обеспечения для совместной работы, трекеры задач), бесшовная интеграция средств разработки, тестирования и развертывания программных продуктов.

В контексте разработки коммерческих программных продуктов, не требующих специальной сертификации, применение гибких методик позволяет работать с короткими релизными циклами (4 и более релиза в год) даже для крупных программных продуктов, однако особенности процедуры подготовки ПО к сертификации вступают в противоречие с фундаментальными принципами «легковесной» разработки (таблица 1).

Таблица 1 – Противоречия между принципами гибкой разработки ПО и требованиями к сертификации

Гибкие методологии	Требования по сертификации
Документация носит ситуативный характер, неконсистентна, фрагментарна, причем элементы обладают различной степенью полноты и дискурсивной связности. Может включать эрративы, семантические, синтаксические и орфографические ошибки специфическую терминологию	Документация выполнена в едином стиле, структурирована согласно ГОСТ 19 серии (ЕСПД), затрагивает конкретные аспекты сборки, настройки и эксплуатации продукта
Потребности заказчика/клиентов имеют высокий приоритет, вследствие чего долгосрочный план носит рекомендательный, а не императивный характер	Все имеющиеся на данный момент функции должны быть документированы, однозначны, непротиворечивы
Разработчик коммерческого продукта может применять актуальные версии инструментов и сторонних программных библиотек, обновляя и заменяя их по мере потери актуальности, нахождения уязвимостей, изменения политик лицензирования	Все программные компоненты, необходимые для компиляции и запуска продукта должны либо входить в дистрибутив (т.е. сертифицироваться совместно с продуктом как библиотеки третьих лиц), либо входить в состав среды выполнения
Процесс сборки может включать в себя обновление исходных кодов и самой среды сборки	Сборка осуществляется в изолированной среде с фиксированным набором инструментов. Обновление исходного кода в процессе сборки не допускается, автоматическое порождение кода нежелательно
Тестирование в среде исполнения производится в типовой ее конфигурации	Тестирование в среде исполнения производится с использованием средств защиты информации

На ранних этапах технологическая цепочка выпуска сертифицированного релиза выглядела следующим образом: 1) производится выпуск коммерческой версии продукта; 2) определяется вид сертификации и требования; 3) производится доработка продукта с учетом требований; 4) производится доработка документации с учетом внесенных изменений; 5) все необходимые артефакты передаются в сертификационную лабораторию; 6) по мере нахождения ошибок производится их устранение и повторная передача обновленных версий продукта и документации; 7) после прохождения соответствующих проверок выдается соответствующее заключение. Если далее требуется сертификация того же релиза в другой системе сертификации или по другим требованиям, цикл начинается заново, однако за счет накопленного опыта производится быстрее. Легко заметить, что этап устранения найденных проблем является итеративным и по своей сути является наименее предсказуемым по возможным временным и трудовым затратам.

Гибридная модель производственного цикла сертифицируемого ПО

Для решения указанных выше противоречий и снижения накладных расходов на подготовку сертифицируемых релизов, предлагается гибридная модель организации производственного цикла, учитывающая зависимость сертифицируемого продукта от базового. Основная идея реализуемого подхода состоит в определении степени этой зависимости и разделении задач по подготовке релизов.

Фактически, весь производственный процесс делится на два этапа, выполняемых коллективами с разными наборами компетенций: 1) выпуск базового продукта осуществляется в режиме принятой в организации гибкой методологии разработки, результатом прохождения этапа являются следующие артефакты: исходные коды продукта, конфигурация сборочной среды и список внесенных изменений; 2) выпуск сертифицированной версии осуществляется на основе полученных от основного производства артефактов путем доработки исходного кода, внесения изменений в среду сборки, сборки продуктов в требуемых условиях, тестирование продукта, доработку документации, передачу

требуемых артефактов сертификационной лаборатории, устранение найденных проблем и, собственно, получение сертификата.

Рассмотрим второй этап более подробно. В свою очередь, в нем можно выделить две стадии, выполняемые последовательно: адаптация сборочной среды вместе с доработкой исходного кода и создание артефактов для сертификации. На первой стадии производится внесение изменений в сборочную среду (добавление возможности отключения несертифицируемых модулей, изолированные сборки и т.п.), при этом от производства необходимо получить конфигурацию среды и исходные коды. Исходные коды размещаются в собственном репозитории, доступ к которому имеют разработчики только сертифицируемого продукта. После получения успешных сборок продукта, он считается готовым к проведению сертификации, конфигурация среды фиксируется. На второй стадии создаются финальные подготовленные сборки, дорабатывается документация, артефакты передаются в лабораторию. Первая стадия выполняется один раз для релиза, в то время как вторая может повторяться итеративно. По мере решения задач, повторяющиеся действия могут быть автоматизированы на более раннем этапе. К примеру, если на каком-либо этапе сборки будет применяться специфический инструмент, например svace, то имеет смысл заранее обеспечить его работоспособность на этапе подготовки среды.

В таком случае зоны ответственности разделяются между специалистами следующим образом: на первой стадии наиболее загруженными являются инженеры, отвечающие за техническую подготовку релиза, а на второй – документоведы и выходной контроль. Данный подход позволяет дать инженерам возможность доработки функциональности сборочных конвейеров, например, реализовав полностью автоматизированную сборку сертифицируемого продукта с нужными параметрами.

Отдельное внимание при внедрении данной модели технологического процесса необходимо уделить документированию. Документацию условно можно разделить на две категории [2]: выходная документация согласно ГОСТ и информационный ресурс, необходимый для обеспечения непрерывного производственного процесса. Такой ресурс может создаваться на базе уже имеющихся средств организации

коллективной работы в связке с трекером задач и включать в себя: лингвистическое обеспечение (глоссарии терминов, указания по именованию артефактов и т.п.), нормативно-правовую базу, описания сборочных сред, инфраструктурных сервисов, процессов сборки, рекомендации по устранению проблем, руководства по развертыванию инфраструктуры. Основным требованием к данному информационному ресурсу является соблюдение его консистентности, непротиворечивости и актуальности.

Для создания выходных документов согласно требованиям ЕСПД в автоматическом может применяться система издательского типа, например на базе LaTeX, обеспечивающая возможность повторного использования текстовых фрагментов в различных документах [3]. Такая система может быть интегрирована со средствами автоматизированной сборки и получать из нее в автоматическом режиме необходимые данные – списки файлов, контрольные суммы и т.п.

Выводы

Обеспечение непрерывности поставок сертифицированного программного продукта представляет собой комплексную проблему, требующую принятия организационно-технических мер, направленных на снижение временных и операционных издержек на доработку базового продукта согласно требованиям безопасности. Для решения данной проблемы была разработана гибридная модель производственного цикла, позволяющая выделить операции, выполняемые в процессе подготовки к сертификации и оптимизировать их с точки зрения трудозатрат за счет выявления повторяющихся однотипных действий. В настоящий момент модель находится в фазе апробации.

Литература:

1. *Мелихов А.А.* Проблематика применения методов автоматической обработки текстов в системах предотвращения утечки данных / Информационная безопасность: вчера, сегодня, завтра: Сборник статей по материалам Международной научно-практической конференции (23 апреля 2019 г. Москва). – Москва: Российский государственный гуманитарный университет, 2019. – С. 108-114.

2. *Лобанов И.А., Мелихов А.А., Белавкин П.А.* Формирование иерархии синтаксических структур при управлении взаимодействием информационных потоков / Нейрокомпьютеры и их применение: тезисы докладов (13 марта 2018 года Москва). – Москва: Московский государственный психолого-педагогический университет, 2018. – С. 403-405.

Козлов А.Д., Нога Н.Л.

Достоверность информации как элемент обеспечения информационной безопасности и оценка ее уровня

Аннотация: В работе авторы предлагают дополнить основные характеристики обеспечения информационной безопасности информационных систем, включая сложные сетевые структуры, категорией достоверности, как ее важной составляющей.

Ключевые слова: достоверность, информационная безопасность, доверие, уровень достоверности, нечеткая логика

В настоящее время в России поставлена задача широкого внедрения цифровых технологий в различных областях экономики [1,2], включая, в том числе, разработку и внедрение систем с искусственным интеллектом.

Федеральная программа «Цифровая экономика Российской Федерации» определяет, что для решения всего комплекса поставленных задач и достижения указанных целей необходимо развитие и совершенствование основных инфраструктурных элементов цифровой экономики (информационная инфраструктура, информационная безопасность).

Нормативные документы в области информационной безопасности (ГОСТы, РД и др.) направлены на защиту информации от несанкционированного доступа, модификации или потери возможности ее использования. Категории защиты, относящиеся к этим трем типам нарушения безопасности, обычно называют конфиденциальностью, целостностью и доступностью.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите