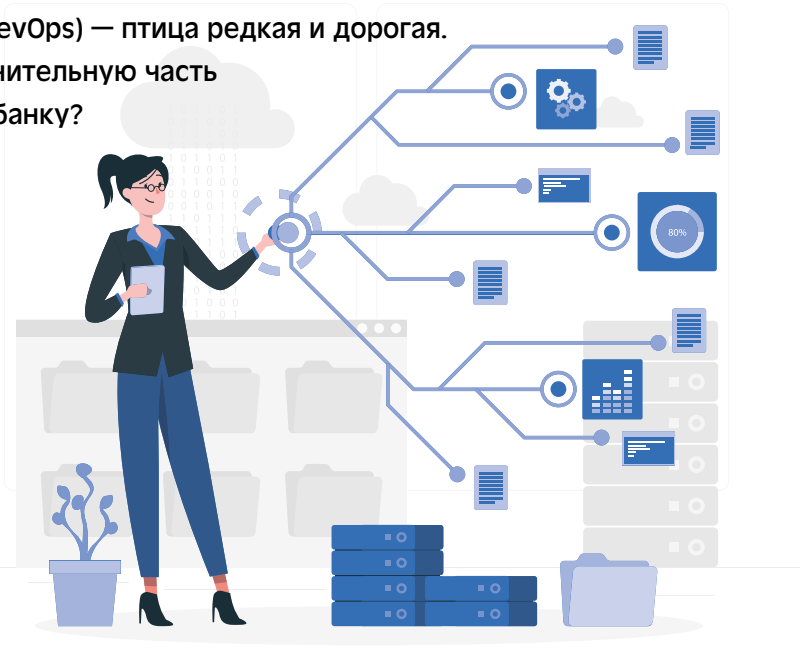
Стратагема работы с микросервисами

Переход на микросервисную архитектуру дает банку многочисленные бизнес-преимущества. Но что происходит, когда банк получает вместо одного монолита множество микросервисов? Его потребность в специалистах по DevSecOps вырастает многократно! Микросервисов в жизни банка все больше, а девопсы (DevOps) — птица редкая и дорогая. В итоге работы по девопсу съедают значительную часть банковского бюджета на IT. Что делать банку?

Текст
ЛАРИСА СТАНКЕВИЧ,
ТЕХНИЧЕСКИЙ ДИРЕКТОР «АРТ-ФИНТЕХ»



В качестве универсального ответа мы, в «АРТ-Финтех», создали экосистему для работы с микросервисами «Автоматический DevSecOps». Наша экосистема помогает успешно решать задачи банка с текущим штатом специалистов, не увеличивая IT-бюджет.

Каждый девопс сможет вести сразу сотни стеков и конфигураций, экономя банку немалые средства. И делать это с легкостью. Как? Расскажу, на что способна созданная нами экосистема.

Основа основ — это работа с репозиториями микросервисов, которая позволяет переиспользовать их. Однажды написанный микросервис оказывается применим для банка внутри разных бизнес-продуктов и конфигураций.

Если банк перешел на микросервисную АБС, он будет работать с тысячами микросервисов. Их надо добавлять, убирать, описывать. Мы создали удобный инструмент, который позволяет добавлять микросервисы и регистрировать их в разных стеках. Этот инструмент, по сути, — средство описания микросервисов и их API.

В инструменте ведения микросервисов и API нет ничего революционного. Некоторые другие решения на рынке тоже помогают создавать такие каталоги. Принципиальное отличие нашей экосистемы от других — в том, что такая каталогизация используется не как справочная информация, а как основа для генерации кода. То есть конфигурация деплоя и организация взаимодействия между микросервисами осуществляются через автоматическую кодогенерацию на основании каталога.

В качестве конфигуратора в «АРТ-Финтех» выступает smART ESB — «умная шина», платформа для управления любыми микросервисами в стиле оркестровки.

Многие банки, работающие на монолитных АБС, уже используют шины. Шины управляют потоками данных, которые передаются между большими системами. Эти потоки крупные, но их количество невелико, — ими легко управлять, используя классические шины.

Когда мы говорим о микросервисной АБС, потоки превращаются в огромное количество «ручейков» обмена данными. Интенсивность обмена возрастает на порядки: в тысячу раз и более. Ни одна классическая монолитная шина не справится с таким количеством «ручейков». Для работы с микросервисами потребовалась микросервисная шина, функционирующая по принципу оркестровки.

Почему банку нужна именно оркестровка и чем она лучше хореографии?

Существует два способа работы шины с данными: хореография и оркестровка. В банках традиционно распространена именно хореография. Хореография означает, что каждый микросервис общается напрямую с каждым, и для этого внутри микросервиса присутствует интеграционный слой.

К чему применение хореографии приводит на практике? Допустим, мы работаем с биллингом и нам надо создать новый тариф. Введение тарифа запросто потребует пересмотреть интеграционный код в десятках или даже сотнях микросервисов. Трудоемкость подобной работы возрастает экспоненциально в зависимости от количества микросервисов, и через некоторое время такая микросервисная система становится аномально дорогой в поддержке.

Другой подход к интеграции микросервисов называется оркестровкой — именно его мы, в «АРТ-Финтех», считаем обязательной составляющей успешной современной АБС. В случае с оркестровкой интеграцией занимается отдельный микросервис, в который вынесена логика обмена данными. Когда для выведения нового банковского продукта на рынок потребуется изменить интеграционную логику, это будет достаточно сделать в одном микросервисе, а не в сотне.

Секрет фантастического time to market для продуктов, созданных в АБС «АРТ-Финтех», прост: интеграция осуществляется с помощью автоматической кодогенерации. Если бы интеграционный код пришлось писать руками, мы бы уперлись в скорость работы программистов. В АБС «АРТ-Финтех» интеграции не пишутся в коде, а рисуются с помощью BPM-схем. Изменения в интеграции соответственно тоже вносятся максимально просто и наглядно. Поменять схему интеграции — интуитивно понятная задача.

Создание конфигурации из стеков

В любом банке существует большое количество разнообразной функциональности и огромный набор стеков. Для того чтобы преобразовать различные стеки в среду исполнения, банку снова требуются многочисленные и дорогостоящие DevSecOps-специалисты. Их задачи: создание наборов микросервисов, которые будут работать в рамках стека, сбор конфигураций, создание эндпоинтов для вызова роутов этих конфигураций. Если весь этот труд останется механическим, он будет стоить банку больших денег.

В рамках экосистемы «Автоматический DevSecOps» от «АРТ-Финтех» нам удалось автоматизировать и сбор стеков, и сбор YAML для них. То есть наше решение позволяет сохранять деньги и время не только на самих интеграциях, но даже на сборе стеков для интеграций.

Работа с данными

Это тот самый «Sec» в названии экосистемы «Автоматический DevSecOps». Безопасность работы с данными должна быть обеспечена не только на уровне фронт-офиса и не может ограничиваться микросервисами. Безопасным должен быть сам доступ к источникам данных. В логике работы экосистемы «АРТ-Финтех» можно добавлять любое количество протоколов безопасности, и доступ к данным открывается только после того, как соблюдены все политики безопасности.

Сейчас зачастую работа с данными осуществляется с помощью «инъекций» SQL- или DDL-кода непосредственно в текст кода микросервисов.

Мы, в «АРТ-Финтех», стараемся этого тщательно избегать. В нашей экосистеме есть отдельный слой SQL-сервисов и NoSQL-сервисов, через который и осуществляется доступ к базам данных. Если какие-то данные оформлены как SQL- или NoSQL-сервис, к ним можно добавить неограниченное количество политик безопасности, соблюдение которых будет обязательным для доступа к конечным данным.

Доступ к определенным данным может требовать, например, двухфакторной аутентификации или наличия определенных сертификатов. Это тоже предусмотрено в нашей экосистеме.

Политики безопасности

Прелесть микросервисной АБС — в том, что политики безопасности должны быть универсальными. Как это реализовано? В АБС «АРТ-Финтех» есть отдельный сервис, содержащий политики безопасности. При генерации нового микросервиса к нему применяется необходимый набор политик безопасности.

Мы также создали специальный микросервис, к которому можно обратиться за проверкой политики безопасности. Его можно вызвать отдельно.

Большой бонус в том, что микросервисная АБС «АРТ-Финтех» позволяет использовать — с соблюдением всех стандартов безопасности — не только собственные микросервисы, но и сторонние, созданные командой банка или другими вендорами. Ко всем ним применяются универсальные политики безопасности «АРТ-Финтех».

Ролевая модель

«АРТ-Финтех» предоставляет богатую ролевую модель с расширенными возможностями. За каждой ролью закреплен определенный набор прав доступа. Но у одного пользователя могут быть несколько ролей в системе. Один и тот же человек может входить в нее с разным набором прав доступа в зависимости от решаемых задач. При смене ролей каждый раз автоматически проверяется, разрешена ли данная роль для пользователя.

Наша экосистема может хранить все сертификаты, с которыми входит пользователь. В случае необходимости в системе можно активировать функцию хранения информации о пользовательских устройствах.

Для решения задач современного банка роли не могут быть «прибиты гвоздями», жестко привязаны к конкретному человеку. У наших крупных клиентов нередко проводится реорганизация на уровне департаментов, могут меняться материнские организации, человек может быть повышен в должности. Ну и, конечно, каждый сотрудник периодически уходит в отпуск и берет больничный. В этих случаях его роль может брать на себя временный заместитель. А экосистема «АРТ-Финтех» позволяет гибко, «на лету», модифицировать зависимости между сотрудниками и их виртуальными ролями. Бесшовное добавление новых политик безопасности было бы невозможным без нашей системы автоматической кодогенерации.

Таким образом, решение «АРТ-Финтех» предлагает новое понимание работы DevSecOps в современной микросервисной АБС. Б.О