Когда все вокруг меняется

Процессы безопасной разработки программного обеспечения в банках не теряют своей актуальности. Наоборот, возникают обстоятельства, требующие изучения накопленных лучших практик и состояния дел в сегменте разработки ПО



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**

В исполнение пункта 2 Указа Президента от 30 марта 2022 года «О мерах по обеспечению технологической независимости и безопасности КИИ» Правительством страны 14 ноября 2023 года выпущено Постановление №1912.

Согласно документу с 1 сентября 2024 года субъектам КИИ будет запрещено приобретать и использовать программно-аппаратные комплексы (ПАК), которые не является доверенными. Кроме того, до 1 января 2030 года субъектам КИИ необходимо будет перейти на преимущественное использование доверенных ПАК. Банк России будет отвечать за этот переход в банковской сфере и иных сферах финансового рынка, а также будет частично организовать его для ряда финансовых организаций.

Чем заменим ПАК?

Положение определяет, что ПАК — это радиоэлектронная продукция, в том числе телекоммуникационное оборудование, программное обеспечение (ПО) и технические средства, работающие совместно для выполнения одной или нескольких сходных задач.

Похоже, на этом заканчивается время работы в нашей стране зарекомендовавших себя, хотя и не являющихся доверенными, инженерных систем (Engineered Systems) Oracle — интегрированных, полнофункциональных платформ, разработанных вместе с СУБД Oracle Database и приложениями для более быстрого и экономичного выполнения критически важных нагрузок, в том числе и в финансовой сфере.

Естественно, «под нож» пойдут и решения других вендоров, покинувших отечественный рынок. Однако, действуют меры поддержки отечественных производителей, введенные в силу наличия целого ряда преимуществ оборудования этого типа.

«Приобретение ПАКа сокращает сроки перехода на отечественное ПО за счет минимизации необходимости тщательного тестирования всех составляющих в связке друг с другом. Использование ПАКов позволяет минимизировать риски несовместимости решений между собой, риски несоответствия функциональных и нефункциональных требований. Например, в части производительности», — пояснил гендиректор компании SimpleOne **Сергей Чуканов** в публикации в издании «Ведомости».

Тем не менее, эксперты, опрошенные изданием, отмечают, что несмотря на все преимущества ПАКов, нельзя сказать, что будет заметен дефицит или высокая конкуренция в этом сегменте. Многие даже считают, что спрос сместится в область разработки собственного ПО, которое будет работать на разрозненном и менее производительном оборудовании.

А это значит, отрасль ждет очередной виток интереса к методикам безопасной разработки софта, а также адаптации множества библиотек, написанных, например, на языке программирования Java, для работы в импортонезависимом стеке, для чего нужна отечественная доверенная среда разработки и исполнения кода. Ведь 80% банковских систем используют платформу Java, которая, к счастью, кроссплатформенная, поэтому переход не вызовет сложностей.

Важность безопасных разработок

Применительно к финансовой сфере с ее сложным регулированием и постоянно изменяющимся требованиями тем разработчикам ПО, которые будут исполнять Постановление №1912, впрочем, как и всем остальным, требуется «сверка часов» с регуляторами.

В частности, сессии «Финансовая отрасль: операционная надежность и киберриски» и «Безопасная разработка — лучшие практики и нормативы сезона 2023-2024», в рамках второй межотраслевой Конференции по вопросам регуляторики в сфере информационной безопасности, организованной Ассоциацией АБИСС, дают массу пищи для размышлений и практической работы.

Методики безопасной разработки ПО возникли не случайно. Когда много лет назад компания Microsoft осознала, что качество их кода находится за пределами приемлемых оценок качества, они предложили подход SDLC (Security Development Lifecycle), который стал каноническим в данной области.

Сочетание Application Security (раздел ИБ, отвечающий за безопасность приложений в целом) и SDLC развернуло вектор разработчиков с обнаружения уязвимостей на предотвращение их появления. Традиционный порядок вопросов — «как?» и «зачем?» — стал подвергаться сомнению. Канонический SDLC, получивший свою детализацию в различных методологиях — OpenSAMM (Open Software Assurance Maturity Model), BSIMM (Building Security in Maturity Model), OWASP (Open Web Application Security Project) и др., расставил все по местам.

Какое-то время все эти методики были необязательны. Но со временем они вошли в состав требований отечественных регуляторов.

В презентации **Александра Бакина,** руководителя Группы защиты приложений Центра информационной безопасности компании «Инфосистемы Джет», перечислены некоторые из них. Во-первых, это Приказ ФСТЭК России от 25.12.2017 года №239 «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ», установил три вида требований. Во-первых, требования по безопасной разработке ПО (наличие руководства по безопасной разработке ПО, проведение анализа угроз безопасности информации ПО, наличие описания структуры ПО). Во-вторых, проведение испытаний по выявлению уязвимостей в ПО (статический анализ исходного кода, фаззинг- и динамическое тестирование). В-третьих, требования к поддержке безопасности ПО (наличие процедуры управления дефектами ПО и процедуры информирования пользователей ПО).

Во-вторых, со стороны Банка России в Положениях 719-П, 683-П, 757-П и ГОСТ 57580.1-2017 прописана процедура оценки соответствия по требованиям не ниже ОУД4 (24+ требования доверия к безопасности, включающие требования к проектной, эксплуатационной документации, жизненному циклу разработки ПО, тестированию и оценке уязвимостей). Сказанное относится к ПО, распространяемое клиентам для совершения финансовых операций (ФО).

Ценность представляет экспертное мнение **Александра Моисеева,** эксперта АБИСС, главного консультанта по информационной безопасности компании AKTIV.CONSULTING,

касающегося практик идентификации и управления изменениями элементов критичной архитектуры для финансовых организаций.

Продолжающийся переход финансового сектора на риск-ориентированный подход к управлению ИБ и обеспечению операционной надежности накладывает определенный отпечаток на процессы разработки ПО. В частности, речь идет о бизнес-процессах управления изменениями, конфигурацией, уязвимостями, а также управлении обновлениями.

Выводы, которые эксперт сделал: «Необходима разработка и адаптация методологии разработки под конкретные ФО. Реализация процессов потребует дополнительные ресурсы для взаимодействия с ФинЦерт. Однако цифровизация процессов сократит трудоемкость составления отчетности для Банка России. И, наконец, управление уязвимостями и обновлениями ПО необходимо производить с использованием методологий ФСТЭК».

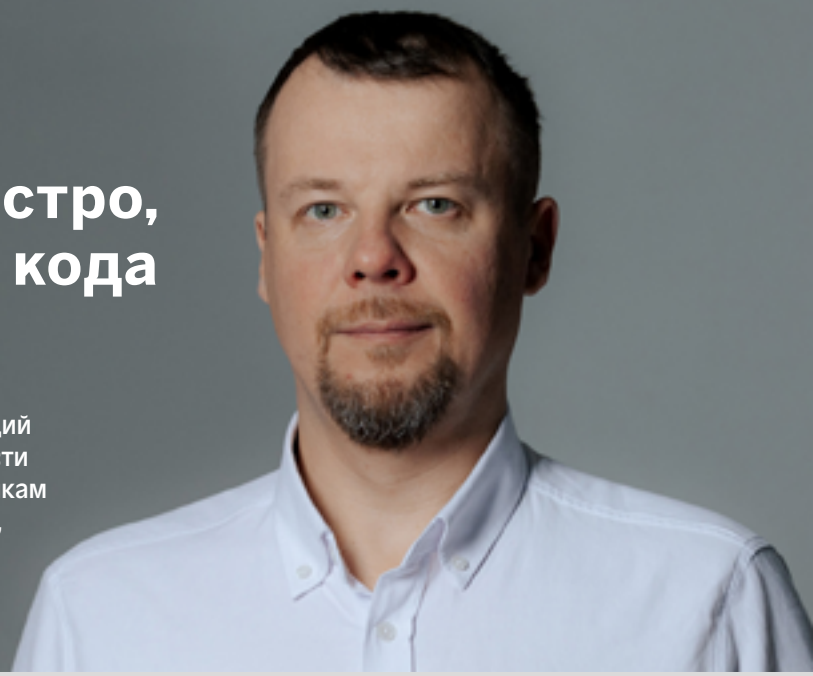
На первый взгляд, может показаться, что набор рекомендаций излишен и непрост к исполнению на практике. Однако пример ведущих банков, оказавшихся в один момент после февраля 2022 года без многих сканеров безопасности (SAST, DAST, SCA и средств сканирования уязвимостей контейнеров и инфраструктуры) и инфраструктурных сервисов (репозиториев, GitOps, CI/CD и система резервного копирования) показал, что основываясь на лучших практиках и грамотном исполнении норм регуляторов, вполне возможно и наладить, и восстановить процессы безопасной разработки ПО.

О свежих лучших практиках области безопасной разработки ПО отлично рассказал на вебинаре RSHB DevSecOps Meetup **Михаил Синельников,** руководитель службы информационной безопасности Россельхозбанка. Запись и презентация эксперта доступна на сайте банка. Поэтому, проблемы с импортозамещением ПАК и альтернативным использованием ПО из их состава, решаемы. Необходимо лишь изучение уже имеющегося опыта, а также помощь консалтинговых и аудиторских компаний.

В заключение необходимо отметить, что Java де-факто продолжает оставаться основной платформой для core-систем, а объем ее кодовой базы — 11 млн строк — сравним с операционной системой. В связи с этим важен опыт организации процессов безопасной разработки в инженерной команде российской платформы Java. Им поделился **Роман Карпов,** директор по стратегии и развитию технологий Axiom JDK: «Для реализации РБПО (разработки безопасного ПО) или SDL необходимы экспертиза и хорошие инструменты. ФСТЭК России всесторонне поддерживает применение самых актуальных технологий анализа программного кода и архитектуры. Наши инженеры используют инструменты ИСП РАН, например статический анализатор Svace. Он объединяет ключевые качества иностранных аналогов с уникальным использованием открытых промышленных компиляторов для максимальной поддержки новых стандартов языков программирования».

По мнению эксперта, внедрение практик РБПО не должно становиться сверхурочной задачей для разработчиков и рушить выстроенные процессы. Это необходимо преподносить как параллельный процесс, плавно интегрируемый в уже устоявшийся ход работ. **Б.О**

Мигрировать на отечественный Java-стек можно быстро, заменив пару строк кода



Одной из важнейших компонент процесса достижения технологической независимости в области разработки ПО для финансовых организаций является достижение функциональной устойчивости и уровня доверия ко всему инструментарию — языкам программирования, компилятору, интерпретатору, средствам разработки и т.д. Обо всем этом «Б.О» рассказал Роман Карпов, директор по стратегии и развитию технологий Axiom JDK

— Какие элементы Security-by-Design среды разработки и исполнения Java Axiom JDK можно выделить?

— Важно разделять безопасность кода среды исполнения Java и приложений, работающих в Java Runtime Environment (JRE). На стороне Axiom JDK для проверки рантайма используется статический анализ и фаззинг. В частности, для фаззинга JIT-компиляторов был разработан собственный инструмент, поскольку не было готовых решений. Для проверки приложений разработчикам также стоит применять анализ зависимостей и статический анализ. Фаззинг поможет выявить уязвимости кода приложения в части обработки входных данных.

И нужно помнить, что далее код должен быть скомпилирован. В случае с Java — это двухуровневая компиляция: в байт-код с применением javac, а далее JIT-компиляция уже непосредственно в виртуальной машине Java. Важно доверять не только коду, который мы проверили, но и компилятору, в котором он исполняется. Если компилятор не доверенный, то нет гарантии, что в результирующий код войдут необходимые усиления, а значит, растет риск эксплуатации уязвимостей в приложении.

Все продукты линейки Axiom JDK и Libercat создаются в соответствии с концепцией разработки безопасного ПО (РБПО) - отечественное название Secure Development Lifecycle, SDLC. Такой подход обеспечивает безопасность систем на протяжении всего периода разработки и эксплуатации. При реализации РБПО инженерная команда использует ряд профессиональных инструментов: фаззинг, статическое и динамическое тестирование.

— Проходят ли тесты на реализацию спецификаций Java SE?

— Безусловно. Вся продуктовая линейка полностью соответствует спецификации Java SE, это очень важно для банковского сектора, который с недавнего времени включился в процесс достижения цифровой независимости и функциональной устойчивости. Благодаря этому миграция банковских информационных систем с зарубежных продуктов (Oracle, Red Hat) на отечественный Java-стек может быть осуществлена в кратчайшие сроки путем замены пары строк кода.

Еще один продукт — стандартизованный сервер приложений Libercat. Он основан на открытых исходных кодах Apache Tomcat, одного из самых популярных серверов приложений, предназначенного для работы с технологиями Java EE (Jakarta EE). Он является заменой зарубежным Oracle WebLogic, IBM WebSphere и JBoss или Wildfly от Red Hat. А в связке Axiom JDK Pro и Libercat предоставляет комплексное сертифицированное решение для обеих спецификаций Java SE и EE.

— Входят ли технологии Axiom JDK в Единый реестр российского ПО и совместимы ли с другими платформами?

— Мы постоянно инвестируем в сертификацию и подтверждение корректной работы компонент Java-стека. Все наши продукты входят в реестр ПО Минцифры и совместимы с отечественными ОС, СУБД, приложениями, аппаратными и процессорными платформами. Синхронно с Oracle Java выходят шесть релизов и обновлений Axiom JDK Pro в год. И почти каждый инженеры дополняют локализацией в соответствии с российскими нормами.

Линейка отечественных Java-технологий включает среду разработки и запуска Java-приложений Axiom JDK Pro, легковесный Java-контейнер Axiom Runtime Container Pro для создания и эксплуатации банковских информационных систем с применением микросервисов, инструментарий нативной разработки Axiom Native Image Kit Pro, контейнерную ОС Axiom Linux, а также сервер приложений Libercat. Он как и Axiom JDK Certified имеет сертифицированную ФСТЭК версию, которая станет широко доступна в ближайшее время. Поскольку количество систем, написанных на базе классической трехзвенной архитектуры и сервера приложений Java EE/Jakarta EE велико, крайне востребована миграция на отечественный Libercat. Б.О

реклама