DOI 10.37882/2223–2966.2023.04.24

СОВРЕМЕННАЯ ПРОБЛЕМАТИКА УПРАВЛЕНИЯ ИТ-АКТИВАМИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

MODERN ISSUES OF IT ASSET MANAGEMENT IN RUSSIAN FEDERATION

A. Marunko
I. Popov

Summary. Object: to discover current problems in IT asset management sphere and generate possible solutions to these problems.

Methods: search for relevant publications in data bases such as e-Library, "Консультант", Google Scholar and among IT asset management community analysis and their following analysis to discover and systemize current problems in this sphere in Russia.

Findings: nowadays, topics of complex IT asset discovery, new technologies management and import substitution are of current interest in Russia. There are several possible alternative ways to mitigate all of these problem types, but it won't be possible to eliminate them completely in the nearest future both in Russia and around the globe.

Conclusions: while managing IT assets in Russia, one might come across both global and local, connected to geopolitical field, issues. Despite them being irremovable, business entities and the ITAM community should seek their mitigation because it opens up new possibilities for development to the whole Russian IT sphere.

Keywords: IT assets, IT asset management (ITAM), software asset management (SAM), software, software as a service (SaaS), licenses, import substitution.

Марунько Анна Сергеевна
Финансовый университет при Правительстве РФ
marunko.a@yandex.ru
Попов Илья Олегович
Финансовый университет при Правительстве РФ
ilya.pop.2014@yandex.ru

Аннотация. Цель: выявить актуальные для России проблемы в области управления ИТ-активами и сформулировать возможные подходы для их решения.

Методы: поиск и анализ публикаций в базах данных e-Library, «Консультант», Google Scholar, а также в сообществах специалистов по управлению ИТ-активами для выявления и систематизации актуальных проблем, которые испытываются в этой области в России.

Результаты: именно вопросы комплексного обнаружения, управления новейшими технологиями и импортозамещения в последнее время стоят в России особенно остро. Возможны несколько альтернативных путей минимизации все этих видов проблем, однако полностью устранить их в ближайшем будущем вряд ли удастся как в России, так и в мире.

Выводы: при управлении ИТ-активами в России встречаются как глобальные, так и локальные, связанные с текущей геополитической проблемы. И хотя их невозможно пока что устранить до конца, их можно и нужно локализовать, смягчая урон и открывая таким образом новые возможности и направления развития для ИТ-сектора.

Ключевые слова: ИТ-активы, управление ИТ-активами, управление программными активами, ПО, ПО как услуга, лицензии, импортозамещение.

Введение

Управление ИТ-активами — это комплекс бизнес-практик по планированию, учёту и отслеживанию состояния ИТ-активов, а также по управлению их жизненным циклом для оперативного контроля и принятия стратегических решений для ИТ-среды. ИТ-активы включают в себя как программные, так и аппаратные элементы ИТ-инфраструктуры предприятия, поэтому зачастую на практике управление ИТ-активами (или ITAM — IT Asset Management) разделяется на HAM (управление аппаратными активами) и SAM (управление программными активами). То есть, иными словами, ITAM отвечает в том числе за закупку и отслеживание лицензий на ПО, закупку и дистрибуцию аппаратных средств между сотрудниками предприятия, ИТ-аудит и так далее [3].

Материалы и методы

Проведен поиск и анализ публикаций в базах данных e-Library, «Консультант», Google Scholar, а также в сообществах специалистов по управлению ИТ-активами для выявления и систематизации актуальных проблем, которые испытываются в этой области в России. Также был проведен дополнительный поиск информации в научных публикациях и на официальных сайтах соответствующих организаций о доступных решениях для задач управления ИТ-активами в России. По результатам анализа найденной информации были сформу-

лированы возможные подходы к локализации и/или устранению выявленных проблем.

Результаты и обсуждение

С управлением ИТ-активами связан многогранный спектр проблем и вопросов, который пытаются решить во всём мире путём формирования и закрепления наилучших практик в этой области. Проблемы управления ИТ-активами в России его можно разделить на две категории: глобальные проблемы управления ИТ-активами и локальные. Глобальная категория включает в себя общие вопросы, присущие данной сфере независимо от геополитической обстановки; а локальная — отвечает за проблемы, возникающие на конкретном экономическом ландшафте, в данном случае — на российском.

Краеугольный камень всеобщих проблем управления ИТ-активами — это отслеживание используемого ПО: его количество, срок окончания и возобновления лицензий, условия лицензирования [3]. Распространённая на западном рынке практика ИТ-аудита от крупных вендоров вроде Microsoft и Oracle угрозой больших штрафов за лицензионное несоответствие заставила компании обратить пристальное внимание на данную проблему. Вопрос отслеживания лицензий усложняется тем, что у многих компаний не только обычные компьютеры и ноутбуки, для которых лицензионную позицию просто посчитать (например, 1 сотрудник равняется 1 лицензии Microsoft Office), они также располагают такими активами, как сервера и мейнфреймы. Для таких аппаратных средств лицензии рассчитываются в зависимости от моделей и количества процессоров внутри, что требует более внимательного подхода к вычислениям [5].

Также сейчас очень популярны концепции Software as a Service (ПО как услуга) и Infrastructure as a Service (Инфраструктура как услуга), связанные с облачными технологиями. SaaS и IaaS позволяют вендорам поставлять приложения заказчикам удалённо, как правило, на их же облачных сервисах по подписке [3]. Это сильно упрощает борьбу вендоров с неправомерным использованием их продуктов, так как приложение не находится на устройстве пользователя. Однако это усложняет работу ИТАМ-отделов внутри клиентских компаний: становится сложнее отслеживать, как и сколько сотрудников пользуются определённым приложением для будущего расчёта лицензий или подписок. Более того, сотрудники зачастую имеют возможность пробовать и пользоваться ПО, которое они нашли и либо воспользовались пробным периодом, либо оплатили сами [4]. Это может показаться безобидным, но такая практика создаёт серьёзную угрозу информационной безопасности компании. В этом и заключается суть проблемы shadow IT (теневых ИТ).

Таким образом, можно увидеть, как посредственное отслеживание ИТ-активов может привести к множеству других проблем: утечки информации и нарушение безопасности компании; неуспешное прохождение ИТ-аудита вендора и возможность нарушения лицензионных соглашений; недовольные сотрудники, не получающие достаточно инструментов для выполнения своих непосредственных обязанностей. В ближайшем будущем нет никаких причин для смены тенденций и уменьшения числа ИТ-активов у компаний, наоборот — они будут лишь расти как в количестве, так и в разнообразии категорий продуктов. Как следствие, поиск эффективных решений для управления ими — это чрезвычайно актуальная проблема не только в России, но и в мире.

Осенью 2021 года, произошёл инцидент с Log4J, который может послужить хорошим примером, как проблема обнаружения и управления ИТ-активов может проявиться и какой ущерб она может нанести.

Log4J — это инструмент логирования от Apache, написанный на Java. Он основан на открытом исходном коде, и поэтому используется в огромном количестве организаций: Apple iCloud, Steam, Twitter и в прочих, в том числе маленьких проектах. Год назад в Log4J была обнаружена критическая уязвимость: с помощью него и Java Naming and Directory Interface возможно устанавливать и запускать удалённо вредоносный код. В итоге уязвимости был присвоен критический статус CVE-2021–44228, а после была выпущена целая серия обновлений, устраняющих уязвимые места в Log4J [6].

Однако, создание новой безопасной версии инструмента ещё не означает, что многочисленные организации по всему миру скачают и установят его. Так как Log4J — это, по сути, лишь часть комплексной библиотеки, большая часть пользователей даже не знает о том, что их системы нуждаются в срочном патче безопасности. Именно развитая культура управления ИТ-активами компании ответственна за информацию о том, что, где и как используется в ИТ-инфраструктуре. Более того, даже если предприятию известно, что уязвимостью затронуты его устройства и используемые программы, временной промежуток между выходом обновления и его установкой всё равно может быть достаточно большим для того, чтобы злоумышленники успели воспользоваться уязвимостью [8].

Данный пример также затрагивает проблему подхода управления программными активами «Patch + Fix». Если это единственный инструмент для улучшения ПО и устранения уязвимостей в организации, то тогда она становится полностью зависима от вендора и от того, насколько оперативно он выпускает обновления. К тому же, при окончании поддержки приложения

разработчик обычно и вовсе перестаёт обновлять его. Также, так как патчи нацелены в основном на базовую версию приложения, зависимость от них усложняет кастомизацию ПО, к которой, как правило, прибегают многие компании со своими уникальными бизнес-требованиями.

В первую очередь для решения проблемы отслеживания ИТ-активов и лицензий на них необходимо воспользоваться приложениями по менеджменту ИТ-активов, которые позволяют автоматизировать и ускорить эти процессы для ИТАМ-специалистов [5]. Однако стоит учитывать, что приложение для управления должно иметь расширенный учёт используемых SaaS и IaaS инструментов. Обычные приложения для управления, как правило, опираются на «денежный след» в своих расчётах, а SaaS и IaaS программы могут не оставлять его, особенно если ими пользуются децентрализовано, несколько отделов из всей организации [4]. Таким образом, приложение для управления ИТ-активами должно выполнять три главных цели: отслеживать ПО, в том числе «теневое», управлять им и превращать его в полноценное ПО для нужд бизнеса.

После того как такой инструмент имплементирован в компании, ИТАМ-отделу необходимо начать продолжительное наблюдение за всей ИТ-средой и регулярно выявлять следующую информацию о приложениях: кто ими пользуется, когда, для чего и какой тренд использования [3]. Также полезно разделять отслеживаемое ПО по его важности для бизнес-процессов. Данный подход снабдит всех сотрудников информацией о том, какие программы используются в компании и какие подойдут для их потребностей. Это уменьшит число тех программ, которые сотрудники устанавливают сами, когда не могут найти что-то подходящее среди предложений от ИТ-отдела. Более того, станет легче рассчитывать необходимое число лицензий при закупках.

Всё описанное выше поможет обнаруживать и отслеживать ПО, но вернёмся к ситуации с Log4J, который является программной компонентой, а не целым приложением. На данный момент набирает популярность такой концепт как Software Bill of Materials — это список всех «open source» и других сторонних компонент, использующихся в кодовой базе программного продукта [10]. По каждой компоненте SBOM минимально содержит информацию о названии, версии и лицензии. Некоторые форматы обязательным указывают ещё и тип компонента (например, «фреймворк» или «библиотека»). За создание такого списка, разумеется, ответственен разработчик программного продукта. Например, в США все ИТ-проекты для госорганов США должны содержать SBOM, поэтому хотелось бы верить, что эта практика скоро перейдёт и в ПО для частного бизнеса, так как это позволит своевременно обнаруживать в ИТ-инфраструктуре звенья, подверженные кибератакам.

Одна из ключевых проблем управления ИТ-активами, присущих именно России — это текущая геополитическая обстановка, в связи с которой основные вендоры большей части используемого российскими компаниями ПО ушли с российского рынка.

Наиболее наглядным образом текущая ситуация стала достаточно проблематичной после официального ухода из России компании Microsoft, поскольку вместе с прекращением поставок какого-либо ПО, было объявлено также о прекращении обслуживания всех продуктов, лицензия которых подходит к концу. Корпорация Microsoft прекратила продажу не только базовых продуктов — ОС Windows и пакета программ Microsoft Office, но и серверного оборудования и ПО — например, Windows Server. Последствием этого решения стала потеря многими коммерческими компаниями, госучреждениями и образовательными организациями доступа к своим серверам удалённого доступа.

У каждой проблемы есть два типа решения: полное устранение и минимизация ущерба (локализация). В этом конкретном случае полное устранение проблемы невозможно. Решать данную проблему необходимо, применяя метод локализации, так как:

- отсутствует альтернативный поставщик некоторых типов ПО, например, пакетов офисных программ;
- отсутствует альтернативная ОС, которая была бы так же распространена, как варианты с западного рынка;
- отсутствует поставщик альтернативных серверных решений;
- отсутствует поставщик альтернативных облачных решений;
- высокий уровень популярности продуктов зарубежных вендоров среди российских пользователей.

Несмотря на то, что данные факторы могут не полностью отразить ситуацию на рынке ИТ-решений в России и многие похожие программы на самом деле реализованы российскими ИТ-компаниями, большинство такого ПО неизвестно широкому кругу клиентов [9]. Более того, продукты корпорации Microsoft и других зарубежных вендоров создают свои собственные экосистемы — наборы продуктов, способные полностью удовлетворить нужды бизнеса и подавляющие необходимость в каких-либо альтернативных поставщиках ПО. Отечественных «ИТ-экосистем» такого рода пока, к сожалению, нет.

Локализовать проблему отсутствия ИТ-активов, к которым так привыкли российские пользователи, можно несколькими способами:

- найти альтернативу среди разработок отечественных ИТ-компаний;
- создать новое ПО на базе российских ИТ-компаний;
- найти альтернативу на мировом рынке ПО;
- внесение поправок в законодательство.

Первый и второй пункты уже используются на уровне Правительства РФ. Примером тому могут послужить госпрограммы по импортозамещению и развитию ИТ-сектора в России. Одной из таких программ является программа по импортозамещению ПО от Правительства Москвы, в рамках которой было создано несколько технологических платформ для разработки, внедрения и обмена инновациями, предоставлены гранты, льготные кредиты и другие меры поддержки [11]. Данный способ можно назвать основной реализуемой стратегией РФ в рамках решения проблемы импортозамещения ПО.

Далее, можно прибегнуть к поиску альтернативных программных продуктов в дружественных странах: например, в Индии и в КНР. Но при ближайшем рассмотрении выяснилось, что на зарубежном дружественном рынке нет развитых альтернатив, по крайней мере в сфере офисного и серверного ПО [7]. Гораздо более выгодно в долгосрочной перспективе развивать отечественные ИТ-продукты.

Четвёртый возможный способ решения — изменение текущего законодательства. В российском законодательстве существует множество актов, указывающих, что любое программное обеспечение и смежные с ним компоненты являются интеллектуальным продуктом, а также устанавливающих ответственность за использование лицензированных программных продуктов без соответствующего разрешения. Основными можно назвать следующие статьи:

- статья 1225 Гражданского Кодекса РФ, «Охраняемые результаты интеллектуальной деятельности и средства индивидуализации»; [1]
- статья 1259 Гражданского Кодекса РФ, «Объекты авторских прав»; [1]
- статья 1229 Гражданского Кодекса РФ, «Исключительное право»; [1]
- статья 7.12 Кодекса об Административных Правонарушениях РФ, «Нарушение авторских и смежных прав, изобретательских и патентных прав». [2]

Данные акты не позволяют использовать «пиратское» ПО. В текущих геополитических реалиях в эти законы можно было бы внести некоторые изменения касательно тех компаний, которые покинули российский рынок, но реализация таких правок заняла бы достаточно много временных и денежных ресурсов. Более того, такие законодательные изменения, скорее всего, оказались бы недостаточно эффективным решением, поскольку изменение данных актов может противоречить нормам международного права или конфликтовать с другими актами в рамках российского законодательства.

Таким образом, развитие и поддержка отечественных разработок ПО и ИТ-сектора в целом — это действительно самый эффективный и перспективный способ реализации импортозамещения ИТ-активов как для российского бизнеса, так и для частных пользователей.

Заключение

В заключение обоих описанных проблем хотелось бы сказать, что это далеко не все испытания, с которыми сталкиваются и отделы по управлению ИТ-активами, и вся сфера ИТ, но, пожалуй, именно вопросы комплексного обнаружения, управления новейшими технологиями и импортозамещения в последнее время стоят в России особенно остро. И хотя их невозможно пока что устранить до конца, их можно и нужно локализовать, смягчая урон и открывая таким образом новые возможности и направления развития для ИТ-сектора.

ЛИТЕРАТУРА

1. Гражданский кодекс Российской Федерации (часть первая) от 26.01.1996 № 14-ФЗ (ред. от 01.07.2021) // СПС «КонсультантПлюс».
2. Кодекс об административных правонарушениях Российской Федерации от 30.12.2001 № 195-ФЗ (ред. от 16.04.2022) // Российская газета. 2001. № 256.
3. Кашурников С.Н., Евдолюк Ю.М. Технология ITAM как эффективная мера управления рисками в сфере информационных технологий // Проблемы анализа риска. 2019. № 1.
4. Кондакова А.В., Золотухина Е.Б. Анализ преимуществ и недостатков SaaS-технологии (программного обеспечения как услуги) // E-Scio. 2019. № 6.
5. Маслова А.С. Перспективы автоматизации информационного процесса управления лицензиями на программное обеспечение на примере ОАО «ПО «Кристалл» // Современные материалы, техника и технологии. 2017. № 4.
6. Сарсенбаева Ж., Исмагул А.А., Плескачев Д.В. Пути защиты от уязвимости LOG 4J // Наука и реальность. 2022. № 1.
7. Сухарев О.С. Государственное управление импортозамещением: преодоление ограничений // Управленец. 2023. № 1.
8. Шинкарев А.А. Роль программного обеспечения с открытым исходным кодом в современной разработке корпоративных информационных систем // Вестник Южно-Уральского государственного университета. Серия: Компьютерные технологии, управление, радиоэлектроника. 2021. № 2.

9. Шиманковский К.В. Импортозамещение в области программного обеспечения бизнес-аналитики // Международный журнал прикладных наук и технологий «Integral». 2022. № 2.
10. Cybersecurity and infrastructure security agency (CISA USA) — Software bill of materials (SBOM) // Электронный доступ URL: https://www.cisa.gov/sbom (дата обращения 02.03.2023).
11. Официальный сайт Мэра Москвы — Импортозамещение: ИТ-решения // Электронный доступ URL: https://www.mos.ru/city/projects/software/ (дата обращения 09.03.2023).

Финансовый университет при Правительстве РФ