УДК 004.056.5

ГИБРИДНЫЙ РЕЖИМ ФУНКЦИОНИРОВАНИЯ ОБЛАЧНЫХ ПЛАТФОРМ

канд. техн. наук, доц. В. П. КОЧИН, аспирант А. В. ШАНЦОВ
(Белорусский государственный университет, Минск)

Аннотация. *Рассмотрено влияние облачных вычислений на безопасность информационных ресурсов. Определена актуальность проблемы обеспечения информационной безопасности коммерческих платформ виртуализации, особенно для Республики Беларусь. Выделены возможные пути решения проблемы обеспечения информационной безопасности платформ виртуализации. Предложен гибридный режим функционирования облачной платформы, позволяющий минимизировать риски, связанные с отзывом лицензий поставщиками коммерческих платформ виртуализации.*

Ключевые слова: *информационные технологии, информационная безопасность, облачные вычисления.*

В настоящее время информационные технологии являются неотъемлемой частью жизнедеятельности современного общества. Реагируя на потребности общества, в первую очередь в коммерческой сфере, организации начали развертывать информационные ресурсы. Однако затраты на развертывания собственных информационных ресурсов для организаций среднего и малого бизнеса, а также для некоммерческих организаций не всегда являлись приемлемыми. В ответ на это появились облачные вычисления, обеспечивающие низкий порог вхождения при развертывании информационных ресурсов.

С развитием облачных вычислений их применение вышло за рамки исключительно коммерческой сферы, облачные вычисления начали применяться в таких областях как медицина и образование [1–3]. Со временем процесс внедрения облачных вычислений достиг самых консервативных сфер жизнедеятельности общества: национальной безопасности и государственного управления. В качестве примера можно привести Министерство обороны Соединенных Штатов Америки (далее – США), которое выделило 10 миллиардов долларов США на развертывание системы ведомственных облачных вычислений – проект Joint Warfighter Cloud Capability [4].

С ростом популярности информационных ресурсов росли и угрозы информационной безопасности. Внедрение облачных вычислений привело к необходимости пересмотра способов и мер защиты информационных ресурсов. Так, для построения системы защиты информации (далее – СЗИ) облачных вычислений

необходимо применять комплексный подход к построению СЗИ, учитывающий особенности, вносимые облачными вычислениями [5]. В рамках данного подхода, защита информационных ресурсов обеспечивается на различных уровнях, одним из которых является уровень защиты платформы виртуализации.

Защита платформы виртуализации осуществляется путем выявления и устранения уязвимостей в программном обеспечении (далее – ПО). Устранение уязвимостей в ПО платформы виртуализации осуществляется с помощью внесения необходимых изменений и выпуска новой версии ПО для последующего обновления. В зависимости от того, является ли платформа виртуализации коммерческим продуктом или собственным продуктом, на базе решений с открытым исходным кодом, провайдер облачных вычислений будет либо самостоятельно осуществлять поддержку платформы в актуальном состоянии, либо такая поддержка должна осуществляться поставщиком коммерческой платформы.

Популярность и высокий спрос на коммерческие продукты виртуализации объясняется существенной экономией ресурсов, связанной с отсутствием необходимости самостоятельно разрабатывать и осуществлять поддержку платформы виртуализации. Большим спросом пользуются коммерческие платформы виртуализации, такие как Microsoft Hyper-V и VMware ESXi [6]. Данные решения приобретаются совместно с лицензиями, определяющими объемы облачных вычислений (количество аппаратных серверов, процессоров, виртуальных машин) и уровень поддержки (сроки выпуска обновлений и исправлений, уровень технической поддержки). В то же время, необходимость приобретения лицензий является одним из существенных недостатков коммерческих решений.

С точки зрения процессов обеспечения информационной безопасности, наличие лицензии необходимо для поддержания защитных механизмов платформы виртуализации в актуальном состоянии. Следовательно, отсутствие лицензии для коммерческой платформы виртуализации потенциально является угрозой информационной безопасности. Угроза отзыва лицензии заключается в отказе поставщика платформы виртуализации осуществлять ее поддержку. Данная угроза особенно актуальна для центров обработки данных (далее – ЦОД), принадлежащих государственным органам и организациям, или обслуживающих государственные организации. В случае реализации угрозы отзыва лицензии ЦОД лишается поддержки по обновлению ПО платформы виртуализации [7]. Отсутствие доступа к исходным кодам ПО платформы виртуализации не позволит провайдерам облачных вычислений в случае отзыва лицензий самостоятельно внести изменения и обеспечить актуальное состояние защитных механизмов облачной платформы, что в свою очередь приведет к ее уязвимостям перед новыми видами кибератак [8].

На сегодняшний день угроза отзыва лицензии является особенно актуальной для Республики Беларусь, испытывающей санкционное давление [9–11].

К сожалению, непосредственной защиты от данной угрозы нет. Рынок коммерческих платформ виртуализации является устоявшимся и поделен между крупными корпорациями. С учетом объёмов рынка Республики Беларусь, данным корпорациям проще отказать в предоставлении услуг, чем рисковать попасть под санкции. Одним из вариантов выхода из данной ситуации является разработка собственной доверенной платформы виртуализации на основе ПО с открытым исходным кодом. Разработка платформы виртуализации является весьма затратной, и в данном случае целесообразно вести разработку в сотрудничестве с другими государствами. Например, с Российской Федерацией, в развитии средств виртуализации ГК Astra Linux «Брест» [12]. Однако в настоящее время в разумные сроки достаточно сложно осуществить переход существующих ЦОДов на альтернативные платформы виртуализации по ряду причин. Во-первых, их функционал уступает таким платформам как Hyper-V или VMware. Во-вторых, это сопряжено с достаточно серьезными финансовыми затратами. В-третьих, для качественного перехода в штате должны быть специалисты, которые имеют навыки работы как с проприетарными системами виртуализации, так с альтернативными.

Однако, даже при наличии доверенной платформы виртуализации, переход с одной платформы на другую является сложным мероприятием. Сложность перехода с одной платформы виртуализации на другую связана с различием в используемых форматах виртуальных машин (далее – ВМ), а также с различием в реализации механизмов защиты информации платформами виртуализации. Различие форматов ВМ не позволяет осуществлять динамическую миграцию ВМ с одной платформы на другую. Перенос ВМ между платформами будет сопряжен с их остановкой, сменой формата (конвертацией), последующим запуском и отладкой на новой платформе. Отличия в защитных механизмах платформ виртуализации требуют разработки новых конфигураций средств защиты информации.

Для непрерывного функционирования информационных ресурсов облачная платформа должна функционировать в гибридном режиме. Под гибридным режимом функционирования облачной платформы подразумевается одновременное использование коммерческих платформ виртуализации и доверенных платформ. Поддержка гибридного режима функционирования облачной платформы может осуществляться как на временной основе, в процессе смены платформы виртуализации, так и на постоянной основе. Постоянная поддержка гибридного режима функционирования облачного ресурса потребует разделения информационных ресурсов на публичные (коммерческие), выбор облачной платформы для которых осуществляется провайдером исходя из экономической целесообразности, и критически важные информационные ресурсы, для которых платформа виртуализации, или требования к платформе, определяется регулирующими органами и техническими нормативными правовыми актами в области защиты информации [13].

Таким образом, провайдеры облачных вычислений должны учитывать риски, связанные с угрозой отзыва лицензий на коммерческие продукты виртуализации. С целью снижения последствий должна быть предусмотрена возможность функционирования облачной платформы в гибридном режиме на временной или постоянной основе. Выбор между временным или постоянным функционированием платформы виртуализации в гибридном режиме должен осуществляться провайдером исходя из расчета затрат, необходимых на поддержку нескольких платформ, или затрат, необходимых для полного перехода на новую платформу виртуализации.

ЛИТЕРАТУРА

1. Управление программным обеспечением и обеспечение отказоустойчивости IaaS-облака / Ю. И. Воротницкий, В. П. Кочин, В. А. Волчок, А. И. Бражук // Электроника инфо. – 2013. – № 9. – С. 21–24.
2. Кочин, В. П. Управление программными проектами на основе облачного сервиса PaaS суперкомпьютера СКИФ / В. П. Кочин, А. В. Жерело // Электроника инфо. – 2013. – № 9. – С. 35–36.
3. Kochyn, V. P. Designing a secure fail-safe cloud repository of paperworks of students and employees of educational institutions / V. P. Kochyn, A. V. Zherelo // Journal of the Belarusian State University. Mathematics and Informatics. – 2021. – № 3. – P. 104–108.
4. Информационный ресурс Министерства обороны США [Электронный ресурс]. – Режим доступа: https://www.defense.gov/Explore/News/Article/Article/2684754/dod-aims-for-new-enterprise-wide-cloud-by-2022. – Дата доступа: 07.07.2021.
5. Кочин, В. П. Проблемы проектирования комплексной системы защиты информации облачных ресурсов в Республике Беларусь/ В. П. Кочин, А. В. Шанцов// Цифровая трансформация. – 2021. – № 3 (16). – С. 34–39.
6. Информационный ресурс Компании IT-Grad [Электронный ресурс]. – Режим доступа: https://www.it-grad.ru/blog/oblaka-i-virtualizaciya-v-electronnoj-kommercii. – Дата доступа: 07.02.2021.
7. Информационный ресурс Компании VMware, Inc [Электронный ресурс]. – Режим доступа: https://news.vmware.com/releases/vmware-statement-regarding-ukraine. – Дата доступа 05.03.2022.
8. Кочин, В. П. Комплексная система защиты информации облачных ресурсов. / В. П. Кочин, А. В. Шанцов // Комплексная защита информации : материалы XXVI науч.-практ. конф., Минск, 25–27 мая 2021 г. / НП РУП «Научно-исследовательский институт технической защиты информации» – Минск, 2021. – С. 332–334.
9. Council regulation (EU) 2022/355 of 2 March 2022 amending Regulation (EC) No 765/2006 concerning restrictive measures in view of the situation in Belarus // Official Journal of the European Union. – 2022. – Vol. 65. – P. 1–102.
10. Council decision (CFSP) 2022/356 of 2 March 2022 amending Decision 2012/642/CFSP concerning restrictive measures in view of the situation in Belarus // Official Journal of the European Union. – 2022. – Vol. 65. – P. 103–111.
11. Информационный ресурс Министерства финансов США [Электронный ресурс]. – Режим доступа: https://home.treasury.gov/system/files/126/belarus_sovereign_debt_prohibition_directive_1.pdf. – Дата доступа: 02.12.2021.

12. Информационный ресурс ГК Astra Linux [Электронный ресурс]: – Режим доступа: https://astralinux.ru/products/pk-brest/. – Дата доступа 22.04.2021.
13. О технической и криптографической защите персональных данных [Электронный ресурс]: Приказ Оперативно-аналитического центра при Президенте Республики Беларусь, 12 ноября 2021 г., № 195 // Оперативно-аналитический центр при Президенте Республики Беларусь. – Режим доступа: https://oac.gov.by/public/content/files/files/law/prikaz-oac/2021-195.pdf. – Дата доступа 16.11.2021.