УДК 002.6; 004.3; 004.65; 004.7; 004.9

Проблемы проектирования комплексной системы защиты информации облачных ресурсов в Республике Беларусь

Кочин В.П., к.т.н., доцент, начальник центра информационных технологий

E-mail: kochyn@bsu.by

Белорусской государственный университет, пр-т. Независимости, д. 4, 220030, г. Минск, Республика Беларусь

Шанцов А.В, аспирант

E-mail: ShantsovAV@bsu.by

Белорусской государственный университет, пр-т. Независимости, д. 4, 220030, г. Минск, Республика Беларусь

Аннотация. Рассмотрено влияние облачных вычислений на информационную безопасность информационных ресурсов при их переносе или развертывании на облачных платформах. Определена актуальность проблемы защиты информационных ресурсов на облачных платформах, в том числе и для Республики Беларусь, и необходимость построения комплексной системы защиты облачных ресурсов. Выделены основные особенности облачных вычислений, влияющих на защищенность информационных ресурсов, такие как: модель совместной ответственности провайдера и клиентов облака по обеспечению информационной безопасности; защита инфраструктуры облачной платформы провайдером; применение надежной подсистемы идентификации клиентов облака; надежная изоляция виртуальных ресурсов клиентов облака; необходимость изменения архитектуры приложений клиентами облака и использования ими шифрования; взаимодействие провайдера и клиентов облака при организации процедуры аудита, реагирования на инциденты и реализации процедур идентификации и аутентификации в развертываемых услугах. Предложены общие подходы по реализации комплексной системы защиты информации облачных ресурсов.

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

Для цитирования: 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.

Problems of Designing Complex Information Security System for Cloud Resources in the Republic of Belarus

V.P. Kochyn, Ph.D., Head of the Information Technology Department.

E-mail: kochyn@bsu.by

Belarusian State University, 4 Independence Ave., 220030 Minsk, Republic of Belarus.

A.V. Shantsou, Ph.D. student.

E-mail: ShantsovAV@bsu.by

Belarusian State University, 4 Independence Ave., 220030 Minsk, Republic of Belarus

Abstract. The influence of cloud computing on the information security of information resources during their transfer or deployment on cloud platforms is considered. The relevance of the problem of protecting information resources on cloud platforms, including for the Republic of Belarus, and the need to build an integrated system for protecting cloud resources are determined. The main features of cloud computing, affecting the security of information resources, are highlighted, such as: a model of joint responsibility of the provider and cloud clients to ensure information security; protection of the cloud platform infrastructure by the provider; the use of a reliable subsystem for identifying cloud clients; reliable isolation of virtual resources

of cloud clients; the need for cloud clients to re-architect their applications and use encryption; Interaction between the cloud provider and clients when organizing audit procedures, incident response and implementing identification and authentication procedures in deployed services. General approaches to the implementation of an integrated information security system for cloud resources are proposed.
Key words: information technology, information security, cloud computing
For citation: Kochyn V.P., Shantsou A. V. Problems of designing complex information security system for cloud resources in the Republic of Belarus. *Cifrovaja transformacija* [Digital transformation], 2021, 3 (16), pp. 34–39 (in Russian).

Введение. На сегодняшний день облачные вычисления являются одной из наиболее быстро развивающихся областей среди информационных технологий. Все больше предприятий производят миграцию своих информационных ресурсов в облако или сразу используют облачную среду при развертывании информационных ресурсов. В подтверждение этой тенденции можно привести статистику роста общей стоимости рынка облачных вычислений [1]. По данной оценке, уже к 2022 году ориентировочная стоимость рынка облачных вычислений составит более 500 миллиардов долларов США. Безусловно, переход к облачным вычислениям имеет ряд существенных преимуществ для предприятий по сравнению с использованием традиционных подходов. Рассмотрим основные из них. На первом месте здесь – экономический аспект. Появление публичных облаков сделало доступным развертывание собственных информационных ресурсов для небольших компаний и организаций, которые не могли себе позволить аренду или создание собственных центров обработки данных (далее – ЦОД).

В качестве второго аспекта можно выделить повышение доступности ресурсов и их информационную безопасность. Применение облачных технологий дает преимущества при распределении нагрузки в случае DDOS атак. В облаке гораздо проще зарезервировать вычислительные мощности и, в случае необходимости, можно также просто и быстро их нарастить. Также в облаке под один сервис выделяется одна виртуальная машина, что позволяет эффективнее настроить ее брандмауэр отключив все неиспользуемые порты. Помимо этого, виртуальные ресурсы динамичны, для облака частое изменение IP адреса ресурса – нормальная ситуация, что также может затруднить атаки на ресурсы.

Тем не менее, остается множество вопросов обеспечения безопасности облачных ресурсов. В ходе одного из исследований [2], владельцам информационных ресурсов было предложено оценить уровень безопасности при переходе в облако. Выяснилось, что именно этот вопрос беспокоит очень многих. Согласно результатам, наблюдается чрезмерная обеспокоенность: 47% опрошенных очень сильно обеспокоены вопросом облачной надежности, 43% проявляют умеренную тревогу, 5% не имеют об этом никакого представления и только оставшиеся 5% не выражают обеспокоенности и уверены в защищенности своих ресурсов.

Не менее интересной оказалась оценка эффективности модели безопасности периметра для облачных ресурсов, применяемая в ЦОД. По мнению большинства (68% голосов), для обеспечения облачной безопасности, не является достаточным применение стратегии, основанной на организации безопасности периметра, 18% затруднилось ответить.

Для Республики Беларусь вопросы защиты информации облачных ресурсов также являются актуальными [3]. На государственном уровне принято решение о переносе информационных ресурсов государственных ведомств и учреждений на облачные платформы специально созданного республиканского ЦОД [4]. Наравне с государственными органами частные формы собственности также активно используют облачные услуги для бизнеса, предоставляемые республиканским ЦОД или такими компаниями как A1, МТС, IBA, Hoster.by и другими.

Изучение проблемы безопасности облачных ресурсов в Республики Беларусь проводилось рядом авторов. Однако в их работах рассматривались отдельные аспекты обеспечения информационной безопасности, а не комплексный подход к решению данной проблемы. Так, например, проводился анализ моделей аутентификации для облачных платформ [5], рассматривались подсистемы обнаружения и предотвращения вторжений [6, с. 98] [7, с. 127]. В работе [8] описывался процесс синтеза модели информационной безопасности для облачных платформ, предоставляющих «Инфраструктуру в качестве услуги». Целью данной работы является определение особенно

стей облачных вычислений, влияющих на защищенность информационных ресурсов, и обоснование необходимости применения комплексного подхода при построении системы защиты информации облачных ресурсов.

Влияние облачных вычислений на информационную безопасность. Информационная безопасность современных облачных решений не является безупречной [9]. Однако, при правильной конфигурации, облачные ресурсы по степени защищенности не только не уступают традиционным вычислениям, но и могут превосходить по ряду показателей. Существует множество примеров развертывания публичных, гибридных и частных облаков с высоким уровнем защищенности. Для обеспечения надежной защиты информации в облачных ресурсах необходимо рассмотреть особенности обеспечения безопасности информации, связанные со спецификой функционирования облака [10].

1. Существенное изменение в модели угроз и политики безопасности. При использовании публичных облаков провайдер предоставляет облачные ресурсы клиентам, которые в свою очередь обслуживают своих потребителей. В зависимости от модели услуг («Программное обеспечение как услуга» – SaaS, «Платформа как услуга» – PaaS, «Инфраструктура как услуга» – IaaS), обязанности по обеспечению безопасности информационных ресурсов в той или иной степени возлагаются на облачного провайдера, но ответственность за сохранность данных перед конечными потребителями несут клиенты, арендующие ресурсы у провайдеров. Следовательно, изначально при миграции в облако необходимо детально изучить уровень обслуживания, предоставляемый облачным провайдером, имеющиеся сертификаты и аттестаты соответствия, а также политику безопасности облачного провайдера и соблюдения им передовых отраслевых практик в области защиты информации, а также выполнить оценку рисков для размещаемых в облаке активов.

2. Провайдер облака должен обеспечивать надежную защиту инфраструктуры облака и подсистемы идентификации. Под идентификацией здесь понимается доступ к управлению виртуальными ресурсами клиентами облака: остановка, запуск и редактирование виртуальных машин, виртуальных контейнеров, рабочих нагрузок, внесение изменений в загрузочные образы и т.д. Защита инфраструктуры – один из ключевых аспектов обеспечения безопасности в традиционных вычислениях. Хотя облачные вычисления имеют свои особенности, за основу построения системы защиты информации взят традиционный подход.

3. Облачный провайдер при настройке инфраструктуры облака должен рассматривать своих клиентов, как потенциальных нарушителей. Это не означает, что клиенты облачных ресурсов обязательно являются нарушителями информационной безопасности или враждебно настроены по отношению к другим клиентам, имеющим активы на этом же облачном ресурсе. Это один из способов повышения уровня безопасности облака. Взломанные виртуальные машины (далее – ВМ) позволяют злоумышленнику реализовывать новые векторы атаки на ВМ других клиентов. Следовательно, в случае если клиенты облака не будут рассматриваться как потенциальные нарушители, защищенность всего облака будет существенно зависеть от защищенности наиболее уязвимой ВМ.

4. Облачный провайдер должен гарантировать изоляцию данных своих пользователей. ВМ динамичны и могут при необходимости освобождать или запрашивать новые ресурсы. В этом случае провайдер должен гарантировать, что при перераспределении ресурсов накопителей новый пользователь не сможет восстановить данные предыдущего пользователя. Также провайдер должен гарантировать защиту энергозависимой памяти от несанкционированного мониторинга со стороны пользователей, что также может привести к раскрытию информации пользователей облака.

5. Клиентам облака необходимо использовать шифрование для своих информационных ресурсов. Хотя применение шифрования и снижает производительность, но избавляет от целого ряда проблем при хранении данных. При использовании шифрования основным вопросом становится управление ключами. В политике безопасности должно быть определено кто должен управлять ключами: провайдер, клиент или конечный пользователь.

6. Учет особенностей облака при развертывании систем безопасности. Традиционные системы обнаружения (предотвращения) вторжений не смогут эффективно функционировать в облачной среде, так как их датчики не способны отследить трафик, передаваемый между ВМ на одной аппаратной платформе. При развертывании на ВМ брандмауэров, прокси-серверов и других систем безопасности следует учитывать, что ВМ, в основном, не столь производительны как аппа

ратные решения и могут стать узким местом в создаваемой сети.

7. Аудит и реагирование на инциденты. Здесь особенно важно тесное взаимодействие клиентов облака с провайдером, для реализации качественной системы по сбору и обработке данных о событиях в облаке. Как правило, потребуется доработка данной системы с учетом специфики облака. Так, например, журналы аудита должны храниться на отдельном виртуальном устройстве (сервисе). Важно обеспечить своевременность отправки журналов аудита на данное устройство, так как динамичный характер выделения ресурсов ВМ может привести к потери данных аудита при отключении части ВМ. Необходимо предусмотреть специальные идентификаторы ВМ. В отличие от традиционных решений, ВМ не могут быть точно идентифицированы по таким параметрам как IP или MAC адрес. Помимо всего этого, нужно согласовать с провайдером то, какие данные будут доступны для аудита, так как облачные платформы ограничивают доступ клиентов к различным журналам аудита (особенно при использовании облачных сервисов по моделям SaaS и PaaS). При реагировании на инциденты также необходимо согласовать с провайдером зоны ответственности, обязанности каждой из сторон, порядок действий, а также резервные каналы связи, в случае недоступности основных (при атаках отказа в обслуживании).

8. Федеративный доступ. В настоящее время Интернет предоставляет для потребителей множество разнообразных сервисов (услуг). Почти каждый из этих сервисов требует от потребителя прохождение процедуры идентификации и аутентификации, как правило на основании уникального идентификатора и пароля. В тоже время, существенно возросло число взломов аккаунтов потребителей услуг, одна из причин – простые пароли, неустойчивые к атакам по словарю. Для искоренения данной проблемы современные сервисы требуют от своих потребителей задания сложных паролей с высокой стойкостью. Однако это делает крайне неудобным управление многочисленными аккаунтами со сложными паролями. Выход из данной ситуации – модель федеративного доступа. При использовании такой модели доступа облачные клиенты должны определить с кем у них могут быть доверительные отношения. Доверяют ли они процедуру доступа таким информационным ресурсам, как, например, Google, Amazon, Facebook и т.д., или они бы предпочли доверить процедуру доступа облачному провайдеру? Либо у пользователей вообще отсутствует доверие к сторонним ресурсам, и они будут осуществлять процедуру доступа исключительно самостоятельно. Все эти вопросы должны найти отражение в политике безопасности облачных пользователей.

В качестве актуального примера применения модели федеративного доступа можно привести Белорусскую интегрированную сервисно-расчетную систему (далее – БИСРС). БИСРС – комплекс информационных систем и ресурсов, предназначенный для идентификации пользователей (физических и юридических лиц) с применением идентификационных карт (ID-карт) в целях оказания им электронных услуг (в том числе административных процедур). Одним из компонентов БИСРС является единая система идентификации физических и юридических лиц (далее – ЕСИФЮЛ). ЕСИФЮЛ осуществляет процедуру единого входа (идентификацию и аутентификацию пользователей) для всех информационных систем, интегрированных в общегосударственную автоматизированную информационную систему [11].

9. Изменение архитектуры приложений под работу в облаке. Облачные вычисления, в основном, обеспечивают безопасное функционирование для приложений, но, как и в большинстве областей облачных технологий, они требуют соразмерных изменений существующих практик, процессов и технологий, которые не были предназначены для работы в облаке. В частности, для приложений необходимо отслеживать API-интерфейсы на предмет аномальной активности и злоупотреблений, особенно когда приложение развернуто на платформе PaaS. Архитектура приложения должна учитывать ограниченную «видимость» и «прозрачность». Под этими терминами подразумевается, что пользователю, развернувшему приложение в облаке, сбор данных о функционировании приложения (системные, сетевые журналы, мониторинг активности приложения) доступен не в полном объеме.

10. Защита данных при их миграции в облако. В большинстве случаев новым облачным клиентам не захочется осуществлять процесс переноса данных в облако в ручном режиме. Им необходимо убедиться в надежности интерфейсов облачного провайдера, предназначенных для передачи данных.

11. Облачным пользователям необходимо узнать у провайдера, где географически будут размещаться их данные. Этот аспект важен не

только с точки зрения доступности ресурсов пользователей, но и с точки зрения распространяемой юрисдикции, предоставления доступа к данным третьей стороне и т.д.

Заключение. В данной статье рассмотрены особенности защиты информационных ресурсов в облаке. К ним относятся как технические, так и организационные меры. Особое место занимает взаимодействие с облачным провайдером. В тоже время, для облака остаются актуальными традиционные методы защиты информации: защита периметра и инфраструктуры, процедуры контроля и управления доступом, использование шифрования, аудит и другое.

Надежность защиты информации можно сравнить с надежностью цепи, где надежность всей цепи определяется надежностью наиболее слабого звена. Этот факт справедлив и для безопасности облаков, где безопасность информации в облаке, определяется степенью защищенности наиболее уязвимого места. Поэтому система защиты должна иметь комплексный характер. Только в случае применения комплексной системы защиты облака, охватывающей все аспекты безопасности, можно говорить о надежной защите информационных ресурсов.

Список литературы

1. Статистика облачных вычислений и факты [Электронный ресурс]. – Режим доступа: https://hostingpill.com/ru/статистика-облачных-вычислений. – Дата доступа 20.01.2021.
2. Облачная безопасность: обзор отчета Spotlight [Электронный ресурс]. – Режим доступа: https://www.it-grad.ru/blog/oblachnaya-bezopasnost-samoe-interesnoe-iz-otcheta-spotlight-report. – Дата доступа: 17.01.2021.
3. Приказ оперативно-аналитического центра от 28.03.2014 № 26 «Об утверждении Положения об основах использования государственными органами и организациями республиканской платформы, действующей на основе технологий облачных вычислений» с изменениями, утвержденными приказом оперативно-аналитического центра от 16.03.2020 № 80.
4. Указ Президента Республики Беларусь от 23.01.2014 № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий» с изменениями, утвержденными Указами Президента Республики Беларусь от 31.12.2015 № 542, от 16.12.2019 № 461.
5. Вишняков В.А., Гондаг Саз М.М. Модели и средства аутентификации пользователей в корпоративных системах управления и облачных вычислениях. Доклады БГУИР. 2016; 3(97): 111-114.
6. Вишняков В.А., Мурашко Е.А., Прокофьев С.В., Марычев Д.В. Система предотвращения вторжений в корпоративную сеть с использованием технологий виртуализации. Материалы 54-й научной конференции аспирантов, магистрантов и студентов «Инфокоммуникации» БГУИР. 2018.
7. Вишняков В.А., Мурашко Е.А., Петкевич Д.А., Марычев Д.В. Система обнаружения вторжений в корпоративную сеть с использованием технологий виртуализации. Материалы 54-й научной конференции аспирантов, магистрантов и студентов «Инфокоммуникации» БГУИР, 2018.
8. Олизарович Е.В., Бражук А.И. Концептуальные основы анализа моделей информационной безопасности облачных систем класса «Инфраструктура как услуга». Доклады БГУИР. 2019; 6(124): 12-20.
9. Отчет об облачной безопасности Check Point software technologies [Электронный ресурс]. – Режим доступа: https://pages.checkpoint.com/2020-cloud-security-report.html. – Дата доступа: 12.01.2021
10. Руководство по безопасности для критических важных областей облачных вычислений Cloud Security Alliance [Электронный ресурс]. – Режим доступа: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf. – Дата доступа: 12.01.2021
11. О Белорусской интегрированной сервисно-расчётной системе [Электронный ресурс]. – Режим доступа: https://www.mpt.gov.by/ru/o-bisrs. – Дата доступа: 26.01.2021

References

1. Statistika oblachnykh vychisleniy i fakty [Cloud computing statistics and facts]. Available at: https://hostingpill.com/ru/статистика-облачных-вычислений (accessed: 20.01.2021) (in Russian).
2. Oblachnaya bezopasnost: obzor otcheta Spotlight [Cloud Security: Spotlight Report Overview]. Available at: https://www.it-grad.ru/blog/oblachnaya-bezopasnost-samoe-interesnoe-iz-otcheta-spotlight-report. (accessed: 17.01.2021) (in Russian).
3. Prikaz operativno-analiticheskogo tsentra ot 28.03.2014 № 26 [Order of the Operational Analytical Center dated 28.03.2014 No. 26] «Ob utverzhdenii Polozheniia ob osnovakh ispol'zovaniia gosudarstvennymi organami i organizatsiiami respublikanskoi platformy, deistvuiushchei na osnove tekhnologii oblachnykh vychislenii» s izmeneniiami, utverzhdennymi prikazom operativno-analiticheskogo tsentra ot 16.03.2020 № 80 (in Russian).
4. Ukaz Prezidenta Respubliki Belarus' ot 23.01.2014 № 46 [Decree of the President of the Republic of Belarus dated

January 23, 2014 No. 46] «Ob ispol'zovanii gosudarstvennymi organami i inymi gosudarstvennymi organizatsiiami telekommunikatsionnykh tekhnologii» s izmeneniiami, utverzhdennymi Ukazami Prezidenta Respubliki Belarus' ot 31.12.2015 № 542, ot 16.12.2019 № 461 (in Russian).
5. Vishnjakov V.A., Gondag Saz M.M. Models and means of user authentication in corporate management systems and cloud computing. Doklady BGUIR [BSUIR reports]. 2016; 3(97): 111-114 (in Russian).
6. Vishnjakov V.A., Murashko E.A., Prokof'ev S.V., Marychev D.V. Enterprise network intrusion prevention system using virtualization technologies. Materialy 54 nauchnoy konferentsii aspirantov. magistrantov i studentov «Infokommunikatsii» BGUIR [Materials of the 54th Scientific Conference of Postgraduates, Undergraduates and Students «Infocommunications» BSUIR]. 2018 (in Russian).
7. Vishnjakov V.A., Murashko E.A., Petkevich D.A., Marychev D.V. Enterprise network intrusion detection system using virtualization technologies. Materialy 54 nauchnoy konferentsii aspirantov. magistrantov i studentov «Infokommunikatsii» BGUIR [Materials of the 54th Scientific Conference of Postgraduates, Undergraduates and Students «Infocommunications» BSUIR]. 2018 (in Russian).
8. Olizarovich E.V., Brazhuk A.I. Conceptual framework of analysis of information security models of cloud systems of the class «Infrastructure as a Service». Doklady BGUIR [BSUIR reports]. 2019; 6(124): 12-20 (in Russian).
9. Otchet ob oblachnoy bezopasnosti Check Point software technologies [Check Point software technologies cloud security report]. Available at: https://pages.checkpoint.com/2020-cloud-security-report.html. (accessed: 12.01.2021).
10. Rukovodstvo po bezopasnosti dlya kriticheskikh vazhnykh oblastey oblachnykh vychisleniy Cloud Security Alliance [Cloud security alliance's security guidance for critical areas of focus in cloud computing]. Available at: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf. (accessed: 12.01.2021).
11. O Belorusskoy integrirovannoy servisno-raschetnoy sisteme [About the Belarusian integrated service settlement system)

Received: 15.07.2021 *Поступила: 15.07.2021*