УДК 004.056.5

Наседкин П.Н. [1]

[1] *Иркутский государственный университет путей и сообщений, г. Иркутск, Российская Федерация*

ОБЛАЧНЫЕ ТЕХНОЛОГИИ В РАМКАХ СЕРВИСНОЙ МОДЕЛИ ОКАЗАНИЯ УСЛУГ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. *В статье рассматриваются особенности и влияние облачных технологий на повышение качества и снижение стоимости затрат в рамках сервисной модели оказания услуг по защите информационных активов предприятий. Рассматриваются основные направления развития услуг и платформ облачных технологий с точки зрения оптимизации затрат, системы управления рисками и обеспечения конфиденциальности, целостности и доступности информации при ее обработке с использованием облачных сервисов.*

Отмечается преимущество планирования затрат на приобретение облачного сервиса по сравнению с «классической» схемой планирования затрат с созданием интегрированной системы управления рисками в рамках выполнения семейства стандартов, касающихся риск - ориентированного управления организацией (ISO 31000), включая обеспечение конфиденциальности, целостности и доступности информации при ее обработке с использованием облачных сервисов.

Проведенный анализ основных направлений развития услуг и платформ облачных технологий показал не только основные достоинства перехода и интеграции IT – инфраструктуры предприятия с облачными решениями, но и обеспечение полной информационной защиты активов предприятия без потери уровня сервиса.

Ключевые слова: *облачные технологии, планирование затрат на безопасность информационных активов, управление информационной безопасностью с использованием облачных технологий. конфиденциальность, целостность и доступность при использовании облачных технологий.*

Nasedkin P.N. [1]

[1] *Irkutsk State University of Railways and Communications, Irkutsk, Russian Federation*

CLOUD TECHNOLOGIES WITHIN THE FRAMEWORK OF THE SERVICE MODEL FOR RENDERING INFORMATION SECURITY SERVICES

Abstract. *The article discusses the features and impact of cloud technologies on improving the quality and reducing the cost of costs in the framework of the service model for the provision of services for the protection of information assets of enterprises. It discusses the main directions of development of services and platforms of cloud technologies in terms of cost optimization, risk management system and ensuring the confidentiality, integrity and availability of information when it is processed using cloud services.*

The advantage of planning the cost of acquiring a cloud service is noted in comparison with the "classical" cost planning scheme with the creation of an integrated risk management system within the framework of the implementation of the family of standards relating to risk-based management of the organization (ISO 31000), including ensuring confidentiality, integrity and availability processing using cloud services.

The analysis of the main directions of development of services and platforms of cloud technologies showed not only the main advantages of the transition and integration of the company's IT infrastructure with cloud solutions, but also ensuring full information protection of the company's assets without loss of service level.

.**Keywords:** *cloud technologies; planning for the security of information assets; management of information security using cloud technologies. confidentiality, integrity and availability when using cloud technologies.*

Введение

Модель обеспечения повсеместного и удобного сетевого доступа к вычислительным ресурсам (сетям передачи данных, серверам, устройствам хранения данных, приложениям и сервисам) с применением облачных информационных технологий может значительно уменьшить расходы на информационную безопасность и поддержание инфраструктуры информационных технологий предприятия. В облачных технологиях выделяют три направле-

ния: программное обеспечение как услуга (SaaS), инфраструктура как услуга (IaaS) и платформа как услуга (PaaS). В области виртуализации растет популярность «контейнеров», когда заказчик получает в аренду изолированную среду для выполнения приложений или процессов со всеми необходимыми компонентами и настройками. Данная услуга занимает промежуточное положение между IaaS и PaaS. Контейнеризация используется как разработчиками новых облачных сервисов, так и разработчиками корпоративного программного обеспечения, поскольку обеспечивает быстрое развертывание и горизонтальное масштабирование приложений. В рамках облачных технологий имеет место развитие гиперконвергентных платформ, которые позволяют объединить в рамках универсального стека вычислительные комплексы, системы хранилищ данных (далее – СХД) и общей сети хранения данных SAN. Такую унифицированную архитектуру легче масштабировать, кроме того, упрощается процесс администрирования.

Программное обеспечение как услуга (SaaS). Программное обеспечение как услуга (SaaS) - это программное обеспечение, которое не нужно устанавливать себе на компьютер, его можно использовать через интернет (пример — электронная почта, Google Docs, системы документооборота, сервисы для организации совместной работы и общения с клиентами). Согласно опросу, проведенному CNews в 2018 г. среди представителей крупного бизнеса, наиболее часто по облачной модели используются решения CRM (33%), а также системы электронного документооборота (28%) и бухгалтерские системы (26%) [3]. В настоящее время темпы роста SaaS не так высоки, как у IaaS и PaaS, но за счет того, что рынок SaaS значительно больше, то это ведет к тому, что традиционные поставщики корпоративного программного обеспечения рано или поздно вынуждены будут преобразовать свою модель потребления, как на основе SaaS.

Инфраструктура как услуга (IaaS). С помощью услуги (IaaS) можно не хранить информацию на компьютере и жестком диске, а размещать их в облаке. Компании, предлагающие данный вид сервисных услуг устанавливают у себя огромные системы хранилищ данных и продают в них места. Предприятие, купив объем памяти у таких компаний загружает свои данные в СХД и получает к ним доступ по сети. В настоящее время на рынке услуга (IaaS) находится в стадии становления и развивается высокими темпами. Среди причин столь быстрого роста отмечаются: рост и предоставление новых облачных услуг (сервисы Microsoft Azure из облака МТС, BDaaS-решение по облачной обработке больших данных и т.п.), а также рост спроса на защищенную облачную инфраструктуру в соответствии с требованием от 27.07.2006 № 152-ФЗ «О персональных данных» на уровне не менее УЗ1 уровня значимости для информационных систем персональных данных (далее – ИСПДн). Облачные платформы и среды виртуализации позволяют быстро выделять необходимые ИТ-ресурсы. Для Disaster Recovery (далее – DR) важна возможность быстрого восстановления виртуальных машин и данных. Облачные технологии и виртуализация отлично подходят для этой цели. Можно создавать очень экономичные решения IaaS – «активный/активный» или «активный/пассивный», т.е. активные узлы обслуживают запросы, тогда как пассивные находятся в «горячем» резерве. Например, задается регулярное резервное копирование виртуальных машин и данных в Центр обработки данных (далее – ЦОД) провайдера. В случае аварии развертывается новая среда – запускаются виртуальные машины с их резервированными данными. Процесс это не мгновенный, но достаточно быстрый. В IaaS главное – гибкость. При реализации стратегии DR провайдер поможет заказчику извлечь из этой гибкости максимум.

Платформа как услуга (PaaS). Эта технология позволяет создавать свои программы с помощью облачных технологий без установки оборудования и специального программного обеспечения. В связи с чем, затраты для предприятия составят только как стоимость за используемые ресурсы (аренда оборудования). С помощью услуги (PaaS) потребитель может создавать свои приложения на основе операционных систем Windows и Linux, обработку и хранение данных которых будет обеспечивать данная облачная платформа.

Планирование затрат на безопасность информационных активов.

С учетом использования облачных технологий общие ежегодные затраты на информационную безопасность предприятия с учетом оптимизации затрат по информационной безопасности формируются, как упрощенная модель трех составляющих компонент (см. рис. 1) [4].

Рис. 1. Категории затрат на безопасность информационных активов

Суммарные ежегодные затраты на информационную безопасность можно рассчитать по формуле (1):

$$ЗИБ = Зо + Зт + Зл \text{ , где (1)}$$

ЗИБ – ежегодные суммарные затраты на безопасность, руб.

Зо – затраты на административно-организационные мероприятия, руб. Затраты включают в себя годовой фонд оплаты труда, представительские расходы, расходы на аналитическую и оперативную деятельность, вообще все, что не включается в прямые затраты на приобретение и эксплуатацию материально-вещественного инструментария безопасности;

Зт– затраты на технические мероприятия, руб. Затраты формируемые за счет технического перевооружения и приобретения/эксплуатации материальных фондов;

Зл – затраты на ликвидацию последствий, руб. Затраты включают резервный фонд, закладываемый на случай обстоятельств не преодолимой силы.

Анализ распределения бюджета на информационные технологии и информационную безопасность по данным источника Computer Economics [2] показывает, что значительная доля расходов приходится на оплату труда сотрудников (36 % от всего бюджета на информационные технологии (ИТ) и информационную безопасность(ИБ)), защиту серверов (8,7 %), компьютеров (8,7 %) и инфраструктуру сети передачи данных (8 %).

Стремление предприятий к оптимизации своих затрат (например, затраты на закупку средств защиты информации, оплата труда специалистов, накладные расходы на обеспечение деятельности по ИБ) приводит к тому, что все больше предприятий (организаций) из различных отраслей экономики активно ищут возможности передачи внешним системным интеграторам облачных сервисов отдельных аспектов обеспечения ИБ и ИТ, в том числе использования готовой ИТ- инфраструктуры внешнего поставщика ИТ и ИБ услуг.

Аутсорсинговая модель облачных сервисов позволяет оптимизировать (уменьшить) затраты предприятий за счет пересмотра ежегодно планируемых затрат на аварийное восстановление по сравнению с «классическим» подходом в разрезе показателей: ROI (Return on Investment) – отдача от инвестиций; Payback – окупаемости, т.е. периода времени, необходимого чтобы доходы, полученные в результате инвестиций, покрыли затраты на эти инвестиции; TCO (Total Cost of Ownership) - совокупной стоимости владения активов.

Значительную роль при планировании затрат предприятия на приобретение облачных сервисов оказывает показатель - Total Cost of Ownership. Преимущество планирования затрат на TCO облачной модели по сравнению с «классической» состоит в том, что предприятие приобретает услугу у внешнего системного интегратора облачных технологий, у которо-

го на обслуживании находится большое количество клиентов, и как следствие приобретаются более дешевые внешние ИТ ресурсы и услуги, в том числе:

- услуги: высококвалифицированных специалистов с уровнем компетенций по соответствующим продуктам и международным вендоронезависимым сертификациями;
- Security Operation Center (SOC) интегратора с централизованным сбором и анализом информации о событиях и инцидентах ИБ;
- услуги в рамках договорных отношений на сопровождение сервисов ИБ;
- услуги основанные на концепции «облачных вычислений» (Cloud Computing), позволяющих снизить затраты за счет ресурсов, за которые не надо будет платить;
- услуги на перевод на аутсорсинг не критичных сервисов, позволяющих сократить затраты на обслуживание и тем самым перераспределить бюджет и сконцентрироваться на критичных для бизнеса сервисах (к не приоритетным видам относятся: обслуживание компьютеров и активного сетевого оборудования, поддержка пользователей и аварийное восстановление);
- услуги на использование более гибких схем лицензирования как программного, так и аппаратного обеспечения, а также скидки на поддержку;
- услуги на оптимизацию затрат с учетом консолидации договоров (например, если перевести все расходы на связь (ip-телефония, трафик, видеоконференции, мобильная связь и другие) в один договор, то можно получить большую скидку от поставщика услуг, чем при множестве раздельных договоров);
- использование услуги SLA (SLA, Service Level Agreement), с учетом приоретизации критических сервисов поддержки 24×7 и выборе более дешевых вариантов поддержки 8×5;
- услуги по продаже технологического места (например, стойки) в центре обработки данных для аренды, при этом затраты на каналы связи и организацию безопасного доступа окупаются за небольшой период.

Управление информационной безопасностью с использованием облачных технологий.

Реализуемый в настоящее время комплексный подход к системе управления информационной безопасностью с использованием облачных технологий в соответствии с циклом Деминга и процессного подхода, а также с лучшими практиками управления ИБ (ISO/IEC 27000) [7,8], необходимо рассматривать как:

- передачу отдельных, а возможно и всего спектра услуг и процессов ИБ на аутсорсинг.
- четкое разграничение ответственности сторон, опираясь на формализованную модель процесса с указанием его входов, выходов,
- потребность в необходимых ресурсах, документации и связей с другими процессами управления по ИБ и ИТ.
- С целью объединения схожих процессов систем управления рисками с привлечением облачных технологий на предприятиях, а также снижения затрат на их операционную поддержку и повышения эффективности управления рисками и предотвращения дублирования операций существует потребность выстраивания интегрированной системы управления ИТ - рисками, объединяющей в себе:
- процессы управления рисками ИБ (в соответствии с ISO/IEC 27000 [7,8], 17799 [1], PCI DSS [17], СТО БР ИББС-1.0-2014 [5], СТО БР ИББС-1.4-2018 [6]);
- рисками управления ИТ - сервисами (на основе ISO 20000 [9] и ITIL [12,13,14,15,16]);
- рисками прерывания бизнеса (по стандартам BS 25999 [18,19], BS 25777 [20] и ISO 22301 [11]).

В связи с чем, применение процессного подхода к реализации процессов управления ИТ и ИБ позволит объединить создаваемую на предприятиях интегрированную систему управления рисками в рамках выполнения семейства стандартов, касающихся риск - ориентированного управления организацией (ISO 31000) [10].

Конфиденциальность, целостность и доступность при использовании облачных технологий.

Облачные сервисы предлагаемые в настоящее время в отечественном секторе экономике в настоящее время соответствуют основным требованиям федерального законодательства и требованиям регуляторов, предъявляемых к информационным системам, использующих для хранения и обработки персональных данных и других видов информации.

Доступность. Доступность облачного сервиса зависит от того какую компанию поставщика облачных технологий предприятие выбирает и от того, какая в настоящий момент и в перспективе политическая обстановка в мире. Подход к обеспечению катастрофоустойчивости получил название «резервный ЦОД как услуга» (Disaster Recovery as a Service, DRaaS). DRaaS исключает влияние аварий на бизнес-процессы, обеспечивает бесперебойную работу, а также снимает с клиента многие вопросы материально-технического и организационного характера. Надежность услуг провайдера обеспечивается двумя (или более) географически удаленными дата - центрами, представляющими собой специализированные здания с высоким уровнем надежности. В случае полностью виртуального ЦОД в каждом из них работает экземпляр виртуального дата - центра клиента – основной и резервный. Все изменения в основном экземпляре в реальном времени отражаются в резервном. Выход из строя любого из экземпляров никак не повлияет на работу организации. Когда случается авария, вместо основного дата - центра мгновенно подключается резервный, и все сотрудники и клиенты продолжают работать в обычном режиме. Отказоустойчивые серверные комплексы облачных ЦОД, построенные на базе кластерной технологии одно из решений в необходимом комплексе мер для обеспечения непрерывности бизнеса и служат для решения трех проблем: обеспечения высокого уровня доступности, или готовности, обеспечения высокой надежности, обеспечения масштабируемости.

Целостность. Крупные поставщики облачных сервисов строят свои решения на базе территориально распределенных центров обработки данных с разветвленной сетью собственных магистральных и городских каналов связи. ИТ - компании при организации облачных сервисов обеспечивают высокий уровень защиты данных от несанкционированного доступа и уничтожения. Технологии частных и публичных облаков упростили репликацию между площадками. Процесс репликации может охватывать все виртуальные машины, конкретные базы данных или снимки данных. Кроме того, облачные технологии помогают организациям выбрать наиболее подходящий по финансовым условиям вариант DR – появилась гибкость выбора допустимого времени простоя. То есть нередко можно выбрать приемлемое время простоя и при этом вписаться в бюджет.

Конфиденциальность. В облачном сервисе данные доступны только клиенту.

Заключение

Таким образом, рассмотренный выше переход на аутсорсинговую модель с привлечением облачных сервисов внешних системных интеграторов ведет к повышению качества и снижению стоимости затрат на сопровождение систем защиты информационных активов предприятий и организаций, а также позволяет работать одновременно с облаком и физической IT-инфраструктурой, объединив их в одну сеть. Сочетание общепринятых международных стандартов и сертифицированной отечественной криптографии обеспечивает полную защиту без потери уровня сервиса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р ИСО/МЭК 17799:2005 — «Информационные технологии. Практические правила управления информационной безопасностью».
2. Кадер М. Окупаемость финансовых вложений в сетевую безопасность. Аналитический обзор «Рынок информационной безопасности 2002», подготовленный компанией CNews.ru / Cisco Systems.
3. Лебедев П. Поставки IaaS и SaaS установили новые рекорды. «Обзор: Облачные сервисы 2018» подготовленный компанией CNews Analitycs / cnews.ru (Источник: http://www.cnews.ru/reviews/cloud2018/articles/postavki_iaas _i_saas_postavili_novye_rekordy).
4. Пискунов И. Планирование затрат на информационную безопасность. Подготовленный компанией Anti-Malware.ru. (Источник: https://www.anti-malware.ru/analytics/Technology_Analysis/economic_planning).
5. Стандарт Банка России СТО БР ИББС-1.0-2014 — Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
6. Стандарт Банка России СТО БР ИББС-1.4-2018 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском информационной безопасности при аутсорсинге».
7. ISO/IEC 27000 — Словарь и определения.
8. ISO/IEC 27001 — «Информационные технологии — Методы обеспечения безопасности — Системы управления информационной безопасностью — Требования». Международный стандарт, базирующийся на BS 7799-2:2005.
9. ISO/IEC 27000-1:2018 Information technology – Service management – Part 1: Service management system requirements.
10. ISO 31000:2018 - Risk management – Guidelines (Менеджмент риска. Руководство);
11. ISO 22301:2012, Societal security – Business continuity management systems – Requirements.
12. ITIL Service Strategy («Стратегия сервиса»), ISBN 978-0-11-331045-6.
13. ITIL Service Design («Проектирование сервиса»), ISBN 978-0-11-331047-0.
14. ITIL Service Transition («Передача сервиса»), ISBN 978-0-11-331048-7.
15. ITIL Service Operations («Эксплуатация сервиса»), ISBN 978-0-11-331046-3.
16. ITIL Continual Service Improvement («Постоянное улучшение сервиса»), ISBN 978-0-11-331049-4.
17. PCI DSS (Payment Card Industry Data Security Standard) — Стандарт безопасности данных индустрии платёжных карт.
18. Part 1, «BS 25999-1:2006 Business Continuity Management. Code of Practice», took the form of general guidance on the processes, principles and terminology recommended for BCM.
19. Part 2, «BS 25999-2:2007 Specification for Business Continuity Management», specified a set of requirements for implementing, operating and improving a BCM System (BCMS).
20. BS 25777:2008, «Управление непрерывностью информационных и коммуникационных технологий – Практические правила».

REFERENCES

1. GOST R ISO / IEC 17799: 2005 – «Information technology. Practical rules of information security management».
2. Kader M. Payback of financial investments in network security. Analytical review «Information Security Market 2002», prepared by CNews.ru / Cisco Systems.

3. P. Lebedev. IaaS and SaaS shipments set new records. «Overview: Cloud Services 2018» prepared by CNews Analitycs / cnews.ru (Source: http://www.cnews.ru/reviews/cloud2018/articles/postavki_iaas_i_saas_postavili_novye_rekordy).

4. Piskunov I. Planning for the cost of information security. Prepared by Anti-Malware.ru. (Source: https://www.anti-malware.ru/analytics/Technology_Analysis/economic_planning).

5. Standard of the Bank of Russia STO BR IBBS-1.0-2014 - Standard of the Bank of Russia: «Ensuring information security of organizations of the banking system of the Russian Federation. General provisions».

6. Standard of the Bank of Russia STO BR IBBS-1.4-2018 «Ensuring the information security of organizations of the banking system of the Russian Federation. Information security risk management in outsourcing».

7. ISO / IEC 27000 - Vocabulary and definitions.

8. ISO / IEC 27001 – «Information technology - Security methods - Information security management systems – Requirements». Interstate standard based on BS 7799-2: 2005.

9. ISO / IEC 27000-1: 2018 Information technology - Service management - Part 1: Service management system requirements.

10. ISO 31000: 2018 - Risk management - Guidelines (Risk Management. Guide).

11. ISO 22301: 2012, Societal security - Business continuity management systems - Requirements.

12. ITIL Service Strategy, ISBN 978-0-11-331045-6.

13. ITIL Service Design («Service Design»), ISBN 978-0-11-331047-0.

14. ITIL Service Transition («Service Transfer»), ISBN 978-0-11-331048-7.

15. ITIL Service Operations («Service Operation»), ISBN 978-0-11-331046-3.

16. ITIL Continual Service Improvement (ISBN 978-0-11-331049-4.

17. PCI DSS (Payment Card Industry Data Security Standard) - A standard for data security of the payment card industry.

18. Part 1, «BS 25999-1: 2006 Business Continuity Management. Code of Practice», BCM.

19. Part 2, «BS 25999-2: 2007 Specification for Business Continuity Management», a BCM System (BCMS) speci-fied.

20. BS 25777: 2008, «Information and Communication Technology Continuity Management - Practical Rules».

Информация об авторах

Наседкин Павел Николаевич – инженер по сетевой безопасности Центра связи и электронного документооборота, Иркутский государственный университет путей и сообщений, г. Иркутск, e-mail: nasedkin_pn@irgups.ru

Authors

Nasedkin Pavel Nikolaevich - network security engineer at the Communications and Electronic Document Management Center, Irkutsk State Transport University, Irkutsk, e-mail: nasedkin_pn@irgups.ru

Для цитирования

Наседкин П.Н. Облачные технологии в рамках сервисной модели оказания услуг по информационной безопасности [Электронный ресурс] / П.Н. Наседкин // Молодая наука Сибири: электрон. науч. журн. – 2019. – №2. – Режим доступа: http://mnv.irgups.ru/toma/24-2019, свободный. – Загл. с экрана. – Яз. рус., англ. (дата обращения: 11.06.2019)

For citation

Nasedkin P.N. Oblachnye tehnologii v ramkah servisnoj modeli okazanija uslug po informacionnoj bezopasnosti [Cloud technologies within the framework of the service model of information security ser-

vices]. *Molodaya nauka Sibiri: ehlektronnyj nauchnyj zhurnal* [Young science of Siberia: electronic scientific journal], 2019, no. 2. [Accessed 20/06/19] (in Russian)