DOI 10.36622/1682-7813.2024.27.1.012
УДК 004.056.53

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ СЕРВИСОВ

А.Г. Александров, А.Ю. Петухов, М.Ю. Рытов

Популярность облачных сервисов стремительно растет. На фоне процессов, связанных с импортозамещением, в том числе и в IT-сфере требуются эффективные, качественные решения. Однако тенденции возрастания количества атак на облачные аккаунты постоянно и неуклонно растут. С учетом большого количества поставщиков, платформ, инструментов и сервисов заказчикам необходимо понимать, кто и за что несет ответственность и как обезопасить данные в облачных средах. В данной статье проанализированы различные платформы, выявлены зоны ответственности в них, как со стороны провайдера, так и со стороны клиента. Рассмотрены вопросы, связанные с обоюдной ответственностью сторон, их зонами контроля. В результате определено, что несмотря на наличие различных инфраструктур, различных сертификатов у провайдеров, клиенту необходимо уделять внимание обсуждению вопросов информационной безопасности на этапе заключения договора на предоставление той или иной услуги.

Ключевые слова: облачные технологии, облачные хранилища, защита облачных сервисов, IaaS, PaaS, SaaS, FaaS, CaaS, кибератака.

Введение

Наиболее ценными активами любого предприятия или организации, являются данные о его деятельности. Поэтому обеспечение целостности и защищенности инфраструктуры любого информационного объекта, это одна из приоритетных задач, как на уровне предприятия, так и на уровне государства. Основными трендами 2019-2023 года в области реализации кибератак являлось использование кибероружия в открытых военных операциях [2,5-7]. Кибератакивность в решении различных конфликтов между государствами приобретает одно из решающих значений. А значит, атаки на инфраструктуры будут только увеличиваться и эволюционировать на новых качественных уровнях.

По информации DataLeakage&BreachIntelligence за первое полугодие 2023 года, основными направлениями атак на инфраструктуры предприятий и учреждений, являлись взломы конкретных баз данных и серверов с целью хищения коммерческой информации. Такими действиями было похищено 83% всей информации полученной через взломы, а общий объем утечек значимых данных вырос до 61 миллиона уникальных записей и 2,4 миллиарда неуникальных. При этом основными причинами утечек коммерческой и иной значимой информации в России до февраля 2022 года являлись действия сотрудников компаний и учреждений [2-7].

Естественно, что основными причинами изменения тактики взломов является тенденция, связанная с уходом иностранных поставщиков средств информационной безопасности, в связи с вводимыми санкциями и геополитическими событиями. Российские компании объективно не были готовы к резкому уменьшению объема средств защиты информации и переходу на российские аналоги программного обеспечения и оборудования.

Данную проблему отчасти можно было бы решить путем экстренного перехода к облачному хранению информации. Однако, такие переходы также сопряжены с рядом особенностей, не позволяющих реализовать их в таком авральном порядке. Да и сама по себе облачная технология на факторы безопасности напрямую не влияет, а лишь позволяет использовать имеющиеся в распоряжении провайдера средства экспертизы и соответствующие ресурсы.

Понимая описываемую нами проблему, на уровне государства 1 мая 2022 года был издан Указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Целью данного указа является принятие необходимых мер по защите критически

важных информационных объектов. Для этой цели Указ фактически запрещает возможность закупки ИТ-продуктов для обеспечения безопасности у иностранных компаний, а с 2025 года полностью ее исключает. Также на наиболее значимых объектах вводятся подразделения и ответственные должностные лица по обеспечению информационной безопасности. Предполагается создание центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ [1].

Исходя из вышесказанного, можно сделать вывод о том, что выработка стратегии обеспечения информационной безопасности на законодательном уровне, а также поиск наиболее оптимальных решений в этой сфере выходит на новый качественный уровень. В данной статье мы попытаемся рассмотреть основные аспекты внедрения и использования облачных технологий и некоторые решения в области обеспечения безопасности данных при использовании облачных сервисов, а также вопросы взаимной ответственности поставщиков облачных решений и их клиентов по поводу защиты информации.

Путь решения поставленной задачи

Современными тенденциями в области использования облачных технологий, является абстрагирование от платформенных решений и мощностей. На смену существующей модели On-Premises, ввиду значительных платформенных издержек, активно применяются IaaS − инфраструктура как услуга, PaaS − платформа как услуга, SaaS − программное обеспечение как услуга, MaaS − мониторинг как услуга, FaaS − функция как услуга, CaaS/fPaaS − коммуникация как услуга. Все эти технологии представляют различные уровни абстракции сервиса предоставляемого клиенту. Естественно, что аппаратная часть в этих решениях существует, но все вопросы, связанные с ее работоспособностью, решает провайдер. Именно он обеспечивает реализацию механизмов физического функционирования, вопросы безопасности, обновления и т. п. Следует сказать, что данные решения продолжают развиваться, появляются гибридные модели, сочетающие в себе возможности перечисленных нами выше или акцентирующие работу на одном решении, но с применением возможностей иных моделей. Иными словами, это реализация работы объединенных облачных сервисов по модели «Anything»asaService (XaaS) или «все, что угодно как услуга».

Не смотря на популярность указанных решений, все они имеют определенные особенности, преимущества и недостатки. Это видно из представленной структурной схемы на рис. 1. Например, SaaS предоставляя набор конкретных услуг, не позволяет реализовывать собственные «функции», FaaS, позволяя реализовывать собственные «функции», привязана к конкретной платформе и не позволяет реализовывать переход к другим платформам. CaaS или fPaaS, реализуя контейнерную схему предоставления услуги и тем самым снимая проблемы двух предыдущих решений, делает миграцию и копирование на другую платформу вполне реализуемыми и не вызывающими сложностей. Следует отметить также, что каждое последующее решение призвано увеличить область управления провайдера или поставщика услуг и уменьшить область управления клиента.

Положительной особенностью приведённых решений, является рекордно быстрое разворачивание системы на этих решениях, так как не требуется платформенных решений on-premises, здесь имеется высокий уровень абстрактности и наличие микросегментации. Тем не менее, несмотря на явные положительные аспекты использования данных решений, для них также сохраняются риски обеспечения информационной безопасности. Прежде всего это связано с неминуемым расширением поверхности атаки, так как при реализации указанных авторами решений более активно используются HTTPAPI, имеется подключение значительного расширения внешних и подключаемых источников.

Это могут быть подключаемые сервисы сообщений, облачные хранилища, что, в свою очередь, сказывается на расширения цепочек

поставки, а, значит, неминуемо влияет на возможность встраивания вредоносного программного обеспечения в эту цепочку. В качестве возможных рисков следует так же выделить риски публичного репозитория и наследования уязвимого кода.

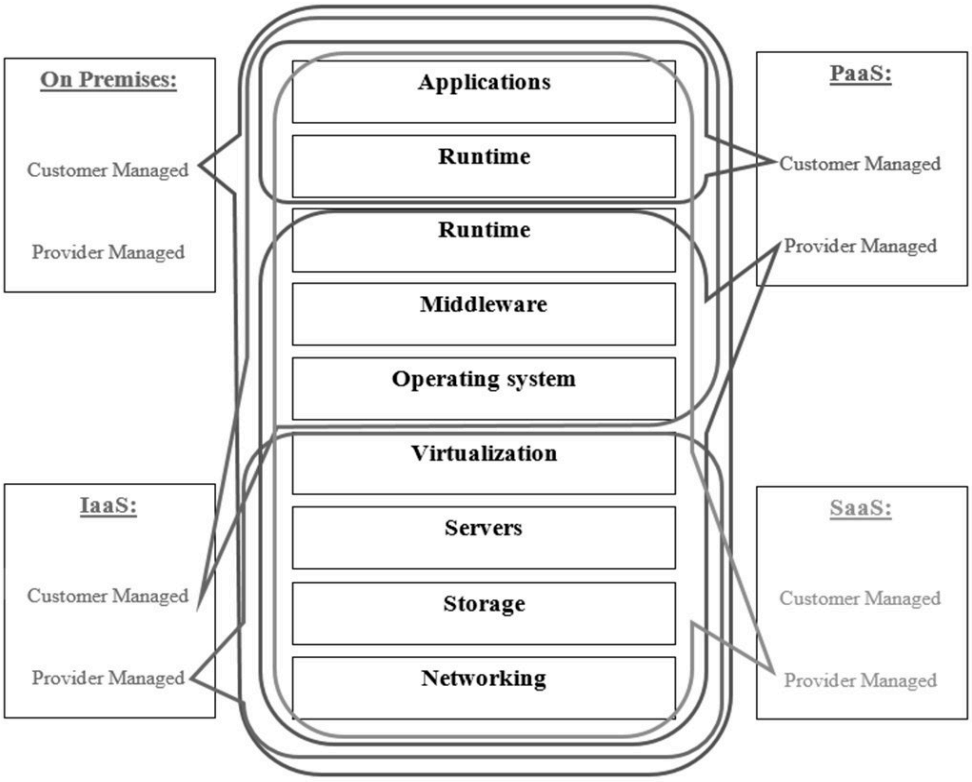

Рис. 1. Структурная схема облачных решений

При условии, что количество облачных миграций с каждым годом будет увеличиваться, вопросы информационной безопасности, будут достаточно серьезной темой для бизнеса и провайдеров. По-прежнему, основными инцидентами являются: массовые утечки данных и последующие атаки скомпрометированными данными, шпионское программное обеспечение, шифровальщики, вайперы, социальная инженерия и т.п. Следует отметить, что рынок криминальных услуг в этой сфере приобретает зрелость.

При наличии таких тенденций, закономерным, является вопрос обеспечения информационной безопасности облачной инфраструктуры, но еще более важным вопросом, при увеличении числа атак на сервисы, является предел ответственности провайдера и получателя услуги - клиента. С учетом того, что количество атак на облачные аккаунты растет гигантскими темпами, необходимо определить эти зоны ответственности. Специалисты утверждают, что 95% отказов безопасности инфраструктуры, вызываются ошибками со стороны клиентов [2, 3, 7].

Клиент, приобретая возможность хранить и обрабатывать информацию в облачной инфраструктуре, обычно полагает, что и вопросы безопасности информации будут возложены на провайдера. Однако, вышеприведенная статистика противоречит данному тезису. Услуги обеспечения информационной безопасности достаточно сложно измерить количественно. Как правило, сегодня оценивается лишь степень соответствия установленным законодательным требованиям. В тоже время, само законодательство и действующие в области информационной безопасности стандарты, подразумевают наличие финансовой ответственности сторон [3, 7].

Очевидно, что вопрос именно разграничения ответственности сторон (провайдера и клиента) является достаточно важным элементом этих правоотношений. Разграничение данной ответственности видится в определении зон ответственности при заключении договора о предоставлении

инфраструктуры между заинтересованными сторонами. При классической схеме обычно по критерию контроля разделяют подобные зоны ответственности. Кто контролирует определенную зону, тот и полностью обеспечивает ее безопасность. Обычно в данном случае следует учитывать наличие так называемых «серых зон», которые не контролируются ни одной из заинтересованных сторон. В таком случае применяется принцип принятия решений. Кто принимает решение на стыке контролируемых зон, тот и несёт ответственность за безопасность информации [3, 7].

Вопросы ответственности провайдера и клиента

Рассматривая приведенные нами виды услуг можно проанализировать разграничение ответственности провайдера и клиента. Для IaaS характерно, что поставщиком услуги предоставляются лишь мощности для функционирования данной услуги. Естественно, что в этой части провайдер обязан обеспечивать физическую безопасность данных, безопасное функционирование сети, которая определяет функционирование облака, безопасные сетевые взаимодействия с другими поставщиками услуг и глобальным Интернетом. Также на поставщика услуги возлагается обязанность по поддержанию в безопасном состоянии среды виртуализации и функциональных систем облака, антивирусной защиты, защите от несанкционированного доступа. Помимо этого, провайдер должен обеспечить безопасное управление доступом своих администраторов, защиту их рабочих мест, сбор и хранение логов созданным облаком, он решает вопросы, связанные с обновлением программного обеспечения для функционирования облака, выявляет и устраняет уязвимости на уровне контроля облака.

В свою очередь, клиент, пользуясь услугой IaaS, получает виртуальные мощности, в пространстве которых он разворачивает свои виртуальные машины и в которых использует свое собственное программное обеспечение для нужд своих пользователей. Очевидно, клиент в этой части, также должен нести ответственность за обеспечение информационной безопасности. Разумно, что такими обязанностями будут являться, защита доступа в сеть Интернет, антивирусная защита собственных виртуальных машин и программного обеспечения, исследование уязвимостей к имеющимся виртуальным машинами и их устранение, настройка доступа пользователей к информационным системам и его контроль, обеспечение обновляемости собственных компонентов системы, сбор и хранение логов собственной системы, контроль за действиями пользователей, шифрование данных.

Не регулируемой и требующей уточнения зоной ответственности здесь является технологическая часть. Как мы уже говорили выше, в таких зонах применяется принцип принятия решений. Кто принимает решение на стыке контролируемых зон, тот и несёт ответственность за безопасность информации. Для обеспечения информационной безопасности таких серых зон необходимо оговаривать отдельно вопросы разграничения и управления доступом сотрудников клиента в центр обработки данных, вопросы межсетевого экранирования, резервного копирования, хранения и обработки логов системы клиента, шифрование жестких дисков, вопросы защиты при администрировании виртуальных машин и программного обеспечения клиента непосредственно в облаке.

Несколько иначе выглядит ситуация при использовании услуги PaaS, где помимо виртуальных мощностей клиенту предоставляется некоторое программное обеспечение для работы с данными уже развернутое в облаке. Здесь, безусловно, провайдер будет контролировать все, что было нами описано выше для услуги IaaS. Помимо этого, он будет осуществлять контроль за обеспечением безопасного доступа к платформе со стороны своих администраторов, обеспечению защищенности предоставляемой клиенту платформы, контролем за учетными записями пользователей, их актуальностью, политиками безопасности, контролем за

сбором логов, производимых используемой платформой, и их хранению.

Обязанностями клиента будут являться: контроль настроек и конфигураций используемой платформы; контроль за обеспечением доступа своих сотрудников к платформе; логирование в приложениях; контроль за действиями своих пользователей.

В серой зоне оказываются такие вопросы информационной безопасности, как межсетевое экранирование, резервное копирование, обработка логов, применение не стандартных средств защиты.

Когда клиент использует услугу SaaS, предполагается, что провайдер предоставляет программное обеспечение как услугу через Интернет. Очевидно, что в таком предоставлении услуги, провайдер неминуемо берет на себя все вопросы, как связанные с информационным обеспечением, так и с обеспечением информационной безопасности. В этом смысле пользователь передает на откуп провайдеру контроль за информационной безопасностью. Однако, с точки зрения пользователя, полезно знать, как провайдер обеспечивает эту безопасность [3,6].

Иными словами, клиенту достаточно выбрать такую инфраструктуру, которая, по его мнению, обеспечивает надлежащую безопасность, при этом гарантирует необходимое быстродействие и уровень качества. Сложность здесь заключается в использовании различных стандартов.

Несмотря на то, что Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных» определяет ключевые требования к обеспечению безопасности информации, связанной с обработкой персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, ряд действующих стандартов включают в себя положения, позволяющие значительно повысить информационную защищенность. Здесь можно привести в качестве примеров стандарты PCI DSS и ГОСТ Р 57580.1 значительно более продвинутые, чем 152-ФЗ. Так что облака, соответствующие этим стандартам, при прочих равных можно считать более защищенными. Соответственно, провайдер выполняющий требования того или иного стандарта, будет предлагать различные «уровни» обеспечения информационной безопасности.

Выводы

На основе вышеизложенного можно сделать вывод о том, что несмотря на различные инфраструктуры, наличие соответствующих сертификатов у провайдера, пользователю необходимо уделять внимание обсуждению вопросов информационной безопасности на этапе заключения договора на предоставление той или иной услуги.

Вопросы ответственности за обеспечение защиты информации, как показывает практика, должны быть оговорены на этапе заключения договора на оказание услуги. Это значит, что на этом этапе необходимо достаточно подробно описывать процедуры управления информационной безопасностью, вопросы урегулирования инцидентов и взаимного контроля и ответственности между собственником и провайдером, обрабатывающим информацию.

Список литературы

1. О дополнительных мерах по обеспечению информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 01.05.2022 № 250 // Официальный интернет-портал правовой информации URL: http://publication.pravo.gov.ru/Document/View/0001202205010023?index=0&rangeSize=1 (дата обращения 10.02.2024).

2. Актуальные киберугрозы: итоги 2022 года // Сайт компании positivetechnologies/ URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения 10.02.2024).

3. Разделение ответственности за обеспечение безопасности в облаке // Сайт Корпоративный облачный провайдер Cloud4Y. URL: https://www.cloud4y.ru/blog/razdelenie-otvetstvennosti-za-obespechenie-bezopasnosti-v-oblake/ (дата обращения 10.02.2024).

4. Баркалов Ю.М. Специальные знания, используемы при исследовании

компьютерной информации: учеб. пособ. / Воронежский институт МВД России, 2017. 46 с.

5. Цифровая криминалистика: учебник для вузов / В.Б. Вехов [и др.]; под ред. В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. Москва: Юрайт, 2024. 490 с.

6. Федотов Н.Н. Форензика – компьютерная криминалистика / М.: Юридический Мир, 2007. 432 с.

7. Positive Technologies: какие уязвимости будут главными угрозами в 2023 году URL: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/apt-cloud-atlas-unbroken-threat/ (дата обращения: 30.12.2023).

Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
Krasnodar Higher Military School named after General of the Army S.M. Shtemenko

Брянский государственный технический университет
Bryansk State Technical University

Поступила в редакцию 15.02.2024

Информация об авторах

Александров Андрей Григорьевич – канд. юр. наук, доцент, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, e-mail: ali_a023@mail.ru

Петухов Андрей Юрьевич – канд. пед. наук, доцент, Краснодарское высшее военное училище имени генерала армии С.М Штеменко, e-mail: petuhow-andrey@mail.ru

Рытов Михаил Юрьевич – канд. техн. наук, заведующий кафедрой «Системы информационной безопасности», Брянский государственный технический университет, e-mail: rmy@tu-bryansk.ru

ANALYSIS OF INFORMATION SECURITY THREATS WHEN USING CLOUD SERVICES

A.G. Aleksandrov, A.Yu. Petukhov, M. Yr. Rytov

The popularity of cloud services is growing rapidly. Against the background of processes related to import substitution, including in the IT sector, effective, high-quality solutions are required. However, the trends of increasing the number of attacks on cloud accounts are constantly and steadily growing. Given the large number of vendors, platforms, tools and services, customers need to understand who is responsible for what and how to secure data in cloud environments. This article analyzes various platforms, identifies areas of responsibility in them, both on the part of the provider and on the part of the client. The issues related to the mutual responsibility of the parties and their control zones are considered. As a result, it was determined that despite the presence of various infrastructures, the availability of various certificates from providers, the client needs to pay attention to discussing information security issues at the stage of concluding a contract for the provision of a particular service.

Keywords: cloud technologies, cloud storage, protection of cloud services, IaaS, PaaS, SaaS, FaaS, CaaS, cyber attack.

Submitted 15.02.2024

Information about the authors

Andrey G. Alexandrov – Cand. Sc. (Law), Associate Professor, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko, e-mail: ali_a023@mail.ru

Yurievich A. Petukhov – Cand. Sc. (Pedagogical), Associate Professor, Krasnodar Higher Military School named after General of the Army S.M. Shtemenko. e-mail: petuhow-andrey@mail.ru

Mikhail Y. Rytov – Cand. Sc. (Technical), Head of the Department of Information Security Systems, Bryansk State Technical University, e-mail:rmy@tu-bryansk.ru