А. А. Шульга, А. А. Оленников
Тюменский государственный университет, г. Тюмень
УДК 004.056.5

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ОБЛАЧНОГО СЕРВИСА ОБРАБОТКИ КОЛИЧЕСТВЕННЫХ ДАННЫХ

Аннотация. В работе анализируется безопасность облачных сервисов для обработки и анализа больших объемов данных. Рассмотрев виды облаков, мы сконцентрировались на особенностях их безопасности. Изучив примеры облачных сервисов для обработки и анализа количественных данных, мы выделили риски, которым они подвержены. Результатом работы являются меры для обеспечения безопасности облачного сервиса обработки количественных данных, основанные на выявленных угрозах.

Ключевые слова: облачный сервис, безопасность данных, обработка количественных данных, типы облачных сервисов.

Введение. Появление облачных технологий сильно повлияло на то, как предприятия и организации хранят и обрабатывают данные. Облачные сервисы предоставляют экономически эффективные решения для обработки больших объемов информации. Тем не менее, с увеличением использования облачных сервисов растут опасения по поводу безопасности данных, хранящихся в облаке. По результатам исследования PwC (PricewaterhouseCoopers), 58% респондентов сомневаются в безопасности и сохранности облачных данных [1]. Обеспечение безопасности облачного сервиса количественной обработки данных имеет первостепенное значение для предприятий и организаций. Потенциальные риски, связанные с утечкой данных и кибератаками, могут иметь серьезные последствия, включая финансовые потери, ущерб репутации и юридические проблемы. Следовательно, важно иметь надежные меры безопасности для защиты конфиденциальных данных и обеспечения безопасности облачной службы. Вопрос безопасности облачных вычислений в последние года все чаще поднимается в исследованиях и научных публикациях. Вишняков А.С., Макаров А.Е., Уткин А.В., Зажогин С.Д., Бобров А.В. проводят в своей работе глубокий анализ существующих решений обеспечения безопасности и выявляют различия в подхо-

дах к ней разных моделей облачных сервисов [2]. Этим в своем исследовании занимались и Прудникова А.А. с Садовниковой Т.М., они обозначили проблемы облачных сервисов с точки зрения информационной безопасности [3]. Сахаров Д.В., Левин М.В., Фостач Е.С. и Виткова Л.А. в своем исследовании разбираются с вопросами безопасности, с которыми приходится сталкиваться при проектировании архитектуры облачных сред, и оформляют генерализованную схему организации защищенного доступа к облачной среде [4]. В статье Немировской-Дутчак О.Э., Морозовой Т.А., Кузнецовой Е.Ю., Прониной Е.В. тема безопасности облачных сервисов сужается до обеспечения безопасности информации в производственных информационных системах [5]. Авторы выявляют потребность в принятии нового стандарта для конкретизации возможных угроз облачных технологий. На основе вышесказанного складывается понимание о важности обеспечения безопасности облачных сервисов. Однако мы видим, что авторы рассматривают безопасность облачных сервисов в общем, не принимая во внимание их предназначение. Переходя на облачные сервисы конкретного назначения, нельзя не сказать о работе Загуменнова А.А., Наумовой В.В. и Еременко В.С. [6]. В ней описан разработанный облачный web-сервис многомерной обработки количественных данных для решения широкого класса научных геологических задач. На примере данной работы можно понять, какие технологии подобных сервисов нуждаются в защите. Потому, объектом настоящего исследования становится облачный сервис обработки количественных данных, в частности, его способность безопасно обрабатывать и хранить количественные данные. Предметом исследований являются различные методы и технологии, которые могут быть использованы для обеспечения безопасности этих данных.

Проблема исследования состоит в выборе методов защиты облачного сервиса обработки количественных данных. Все больше организаций и частных лиц принимают облачные решения, появляется необходимость обеспечения безопасности конфиденциальных данных. Количественная обработка данных, включает в себя использование сложных алгоритмов и статистических моделей, которые

могут быть подвержены кибератакам и нарушениям данных. Изучая и реализуя меры для обеспечения безопасности облачных сервисов для количественной обработки данных, мы можем защитить конфиденциальную информацию, предотвратить потерю данных и поддерживать целостность процессов принятия решений, управляемых данными. Задачей данного исследования является выявление наиболее эффективных методов защиты конфиденциальных данных в облачном сервисе обработки количественных данных, что в конечном итоге помогает предотвратить инциденты безопасности, которые могут поставить под угрозу целостность обработанной информации.

Материалы и методы. Для выявления эффективных методов защиты данных необходимо проанализировать существующие виды облачных сервисов. Для начала рассмотрим облачные сервисы по типу предоставляемых услуг. От типа сервиса будет зависеть тип управления данными, то есть какие слои безопасности контролируются клиентом, а какие провайдером. Приложение как сервис (SaaS) работает по принципу предоставления конечному пользователю доступа к приложению, размещенному на серверах провайдера услуги. И потому как управление конфигурацией инфраструктуры, операционной системой и возможностями облачной платформы остается за провайдером, обеспечение безопасности сервиса также лежит на нем. Пользователю предоставляется лишь web-интерфейс, который возможно использовать практически на всех платформах, имеющих браузер. Платформа как сервис (PaaS) предоставляет конечному пользователю возможность размещать на платформе и конфигурировать свои приложения на необходимых ему языках программирования и инструментах. Однако клиенты не могут управлять инфраструктурой облачных приложений и контролировать сеть, сервер, операционную систему, системы хранения данных. Потому в данной модели уже сами пользователи должны уделять внимание безопасности приложений, а также вопросам, связанным с управлением API. В особенности это касается подтверждения прав доступа, проверки и авторизации. Если же потребителю необходим контроль над вычислительными мощностями, конфигурацией облачной платформы, операционной системой и ее установкой, а также необходимыми приложениями, ему подойдет модель IaaS — инфраструктура,

как сервис. Конечный потребитель не контролируется поставщиком, а также, как и в Paas, он сам должен обеспечивать безопасность операционных систем, данных и приложений. Однако, в IaaS встроенны несколько возможностей обеспечения безопасности без защиты инфраструктуры самой по себе [8].

Теперь выявим особенности обеспечения безопасности разных по доступности типов облаков, ведь выбор модели развертывания облачной среды также оказывает влияние на уровень безопасности. Самым надежным считается частное облако. Им пользуется лишь одна компания, она же и будет отвечать за все аспекты безопасности сервиса. Организация будет нести ответственность за инфраструктуру, доступность, а также инциденты информационной безопасности. При этом у нее нет необходимости в доверии к какому-либо провайдеру облачных услуг, ведь только сотрудники компании имеют доступ к облаку. Обычно доступ предоставляется через виртуальную частную сеть. Общественное облако предназначается организациям, имеющим общие проблемы и задачи. Тогда инфраструктура может принадлежать одной или более организациям из образованного сообщества, а за обеспечение безопасности и доступности будут отвечать владельцы облачной инфраструктуры, они же ответственны и за сохранность данных. Облачная же инфраструктура, доступная для открытого использования называется публичным облаком. При таком развертывании за безопасность и доступность отвечает провайдер услуг. Последним типом является облачная инфраструктура, сочетающая в себе описанные выше типы облачных сервисов. Такую инфраструктуру называют гибридным облаком, и в ней все компоненты — самостоятельные платформы, а для доставки запросов к нужному компоненту используются стандартизированные или частные технологии [7].

Следующим вопросом для рассмотрения являются вопросы безопасности облачных сервисов количественной обработки данных. Эти службы обеспечивают предприятиям доступ к мощным компьютерным ресурсам, которые могут выполнять сложные задачи анализа данных. Такой облачный сервис в единой точке доступа предоставляет методы многомерной обработки количественных данных

для решения различного рода задач на основе открытых решений [6]. Облачные сервисы количественной обработки данных обладают несколькими преимуществами по сравнению с традиционными локальными решениями, такими как масштабируемость, экономическая эффективность, гибкость. Несмотря на преимущества облачных сервисов количественной обработки данных, существуют также опасения по поводу безопасности этих услуг. Одной из основных проблем является конфиденциальность. Облачные сервисы количественной обработки данных включают хранение и обработку больших объемов конфиденциальной информации, такой как финансовые и личные данные, интеллектуальная собственность. Эта информация хранится на удаленных серверах, принадлежащих и управляемых сторонним поставщиком облачных услуг. Это вызывает обеспокоенность по поводу безопасности данных, а также конфиденциальности людей, чьи данные хранятся и обрабатываются. Облачные сервисы обработки количественных данных лучше развертывать как публичные, так как ими будут пользоваться сразу несколько заказчиков. И потому как в публичных облаках размещается большое количество данных, они более заманчивы для атак злоумышленников и требуют от провайдера повышенного внимания к безопасности. По типу же предоставляемых услуг такие сервисы относятся к SaaS, клиентам предоставляется удаленный доступ лишь к набору приложений, которыми можно пользоваться. Поэтому детали функционирования сервиса, его инфраструктура оказываются скрытыми для пользователя, а вся ответственность за безопасность сервиса полностью лежит на поставщике. Каким же рискам подвержены данные, хранящиеся в подобных облачных сервисах? Ответим на этот вопрос, взяв за основу список основных угроз в облачной безопасности, представленный на докладе директора компании Huawei по развитию облачных технологий в России, Артура Пярна [9]. Первая угроза это, конечно, утечка информации. Возникнуть она может по вине сотрудников, в результате ошибки в настройках безопасности или при атаке на сервис извне. Так, к утечке данных и компрометации может привести недостаточное управление доступом, авторизацией и учетными данными пользователей. Например, получение пользователем более широких прав, чем ему необходимо

для работы. В результате массового применения разработчиками API протоколов актуальна и угроза небезопасного использование портов и API. Также при анализе безопасности облачных сервисов нельзя не обратить внимание и на инциденты связанные с невосполнимой потерей данных. Развертывая облачный сервис обработки количественных данных как публичное облако, важно учитывать риски использования совместных ресурсов. И конечно, реализуя методы защиты облачных сервисов, необходимо помнить о внешних угрозах, таких как DoS и DdoS проблемы, APT-угрозы и угрозы взлома аккаунтов.

Результаты. После проведения представленного выше анализа, были выявлены наиболее эффективные меры обеспечения безопасности облачных услуг количественной обработки данных. Шифрование — процесс преобразования данных в кодированную форму, которую можно расшифровать только с помощью ключа дешифрования. Шифрование можно использовать как для обеспечения безопасности данных, прежде чем они будут сохранены или переданы в облаке, так и для безопасного хранения скриптов. Для передачи лучше использовать сквозное шифрование (также называемое оконечным шифрованием, end-to-end encryption, E2EE). В отличие от шифрования транспортного уровня, оно передает данные так, что прочитать их могут только отправитель и получатель, которые имеют ключи для расшифровки сообщений. Так сквозное шифрование гарантирует конфиденциальность, ведь никакая третья сторона прочитать зашифрованные данные не может: ни злоумышленники, ни даже сервер, через который проходят данные. Обеспечивает E2EE и целостность, так как с применением алгоритма AES (Advanced Encryption Standard) в режиме GCM (Galois/Counter Mode) незаметно изменить сообщение невозможно, поскольку любая попытка корректировки будет сразу замечена. Однако, для сервисов, которые хотят более высокий уровень защиты ценой небольшой потери производительности больше подойдет относительно новая и развивающаяся технология полностью гомоморфного шифрования. Она позволит совершать необходимые операции, математические действия над данными в облачном сервисе обработки

количественных данных при этом, не раскрывая сами данные провайдеру облака. Такая криптосистема гомоморфна относительно обеих операций — и сложения, и умножения. Гомоморфное шифрование даст возможность сохранить целостность, доступность и конфиденциальность данных при обработке их в облачных системах. Для обеспечения целостности количественных данных, часто представляющих и конфиденциальную информацию необходимо защитить данные от несанкционированного доступа. Для этого надлежит использовать контроль доступа. Он может включать в себя такие меры, как защита пароля, многофакторная аутентификация, а также контроль доступа, базирующийся на ролях (Role Based Access Control, RBAC). Для управления доступом в облачных сервисах лучше использовать Identity and Access Management (IAM) — систему управления пользователями, группами, политиками и ролями. За счет управления учетными записями она позволит снизить риск компрометации и утечки данных, которые возникают при чрезмерно привилегированных правами доступа пользователях. IAM позволит сократить время и ресурсы, необходимые для ручного управления доступом, а также снизит риск человеческих ошибок, что очень важно при работе с большим количеством пользователей облачного сервиса. Резервное копирование данных и восстановление — процесс создания копий данных и их хранения в безопасном месте. Он гарантирует, что, если исходные данные потеряны или повреждены, их можно восстановить из резервной копии. Для обеспечения мобильности среды и быстрого восстановления данных при их утере или повреждении необходимо настроить автоматическое аварийное восстановление. Защить же копии данных можно с помощью облачного резервного копирования. Важно в облачных сервисах обработки количественных данных осуществлять и архивирование. Оно подходит для больших объемов данных, которые могут быть выделены из производственных рабочих мощностей, а также не используются часто.

Заключение. Появление облачных технологий изменило способ, которым предприятия и организации хранят и обрабатывают данные, предоставляя экономически эффективные средства анализа данных. Тем не менее, безопасность облачных вычислений остается

значительной проблемой, ведь до сих пор существуют такие риски как утечка данных и кибератаки, приводящие к серьезным последствиям для производств и предприятий. Следовательно, внедрение надежных мер обеспечения безопасности имеет большое значение. Эта работа предоставила анализ с точки зрения безопасности разных типов облачных сервисов, а также общих принципов работы облачного сервиса обработки количественных данных. На его основе был выявлены такие меры обеспечения безопасности, как шифрование, контроль доступа, резервное копирование и восстановление данных, а также представлены варианты их реализации. Изучая и реализуя эти меры, мы можем защитить конфиденциальную информацию, предотвратить потерю данных и поддерживать целостность процессов принятия решений, управляемых данными. В конечном счете, работа направлена на то, чтобы предоставить информацию и рекомендации по повышению безопасности облачных сервисов, используемых для количественной обработки данных. В будущем же авторами планируется разработать свой собственный сервис обработки количественных данных, важное место уделив именно обеспечению его безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Глобальное исследование Digital Trust Insights 2021. — Текст: электронный // PwS : [сайт]. — URL: https://www.pwc.com/kz/ru/ services/global-digital-trust-insights.html#modules (дата обращения: 10.04.2023).
2. Обеспечение защиты данных, представленных в облачных сервисах / А.С. Вишняков, А.Е. Макаров, А.В. Уткин [и др.]. — Текст: непосредственный // Вестник науки и образования. — 2019. — №. 11-2 (65). — С. 22-29.
3. Прудникова А. А. Анализ облачных сервисов с точки зрения информационной безопасности / А. А. Прудникова, Т. М. Садовникова. — Текст: непосредственный // T-Comm-Телекоммуникации и Транспорт. — 2012. — №. 7. — С. 153-156.
4. Сахаров Д. В. Исследование механизмов обеспечения защищенного доступа к данным, размещенным в облачной инфраструктуре / Д.В. Сахаров, М.В. Левин, Е.С. Фостач, Л.А. Виткова. — Текст: непосредственный // Наукоемкие технологии в космических исследованиях Земли. — 2017. — Т. 9, № 2. — С. 40-46.

5. Немировская-Дутчак О. Э. Обеспечение информационной безопасности при применении облачных технологий в производственных информационных системах / О.Э. Немировская-Дутчак, Т.А. Морозова, Е.Ю. Кузнецова, Е.В. Пронина — Текст : непосредственный // Международный журнал прикладных наук и технологий «Integral». — 2022. — № 5. — С. 1805-1818.
6. Загуменнов А. А. Облачный сервис многомерной обработки количественных данных для решения геологических задач / А. А. Загуменнов, В. В. Наумова, В. С. Еременко. — Текст : непосредственный // Вестник Новосибирского государственного университета. — Серия: Информационные технологии. — 2021. — Т. 19, № 3. — С. 40-49.
7. Нестеренко В. Р. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними / В.Р. Нестеренко, М. А. Маслова. — Текст : непосредственный // Научный результат. Информационные технологии. — 2021. — Т. 6, № 1. — С. 48-54.
8. SaaS, PaaS и IaaS: уровень риска сильно отличается. — Текст : электронный // tadviser : [сайт]. — URL: https://www.tadviser.ru/a/60572 (дата обращения: 09.05.2023).
9. Артур Пярн, Huawei в России о современных вызовах и угрозах ИБ. — Текст: электронный // infoforum.online: [сайт]. — URL: https://infoforum.online/experts-experience/video-artur-pyarn-huawei-v-rossii-o-sovremen (дата обращения: 19.05.2023).