Вопросы безопасности
Правильная ссылка на статью:
Беспалова Н.В., Нечаев С.В. — Обеспечение информационной безопасности облачных хранилищ // Вопросы безопасности. – 2023. – № 2. DOI: 10.25136/2409-7543.2023.2.40770 EDN: INXNVX URL: https://nbpublish.com/library_read_article.php?id=40770

Обеспечение информационной безопасности облачных хранилищ

Беспалова Наталья Викторовна

ORCID: 0000-0003-3733-3119

кандидат физико-математических наук

доцент, департамент Анализа данных и машинного обучения, Финансовый университет при Правительстве Российской Федерации

125167, Россия, г. Москва, пр. Ленинградский, 49/2

NVBespalova@fa.ru

Нечаев Сергей Васильевич

ORCID: 0009-0009-8987-8648

студент, кафедра Информационная безопасность, федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

197101, Россия, г. Санкт-Петербург, пр. Кронверкский, 49/А

sergey.nechaev2018@yandex.ru

Статья из рубрики "Информационное обеспечение национальной безопасности"

DOI:

10.25136/2409-7543.2023.2.40770

EDN:

INXNVX

Дата направления статьи в редакцию:

17-05-2023

Дата публикации:

07-06-2023

Аннотация: Предметом исследования являются облачные хранилища. Объектом исследования является информационная безопасность облачных систем. В ходе работы была определена нормативно-правовая база, которая позволяет регулировать работу с облачными технологиями на законодательном уровне. Были проанализированы

Российские и зарубежные статистические данные по использованию облачных технологий корпоративными клиентами и физическими лицами, определены основные специфические проблемы безопасности облачных решений, такие как, хранение данных, использование в облаке модульной инфраструктуры, уязвимость виртуальных машин к заражению вредоносным программным обеспечением, нестабильность соединения, разграничение прав доступа, несбалансированность действий клиента и поставщика облачных услуг. В ходе работы была сформулирована концепция построения многоуровневой безопасности облачных систем. Такой подход позволит не только увеличить временные затраты, но и трудоемкость процесса проникновения злоумышленника в систему, что повысит шансы своевременного распознавания и предотвращения различного типа атак. Было предложено решение по построению системы безопасности, включающее в себя следующие этапы: выбор надежных методов шифрования и аутентификации, использование межсетевого экрана, с целью фильтрации трафика и предотвращения вторжений, обеспечение передачи данных по сети интернет в защищенном исполнении, использование системы обнаружения и предотвращения вторжений.

Ключевые слова:

информационная безопасность, облачные системы, персональные данные, шифрование, конфиденциальность, целостность, аутентификация, вредоносное программное обеспечение, операционная система, межсетевой экран

Активное развитие современных технологий способствует расширению спектра решений, направленных на повышение эффективности и удобства работы пользователей. Одним из наиболее популярных подобных решений являются облачные системы. К их преимуществам можно отнести:

· доступность информации с любого удобного устройства;

· работа с большими объемами данных;

· относительно низкая стоимость;

· высокий уровень вычислительных мощностей

· гибкая система оплаты услуг. [1]

Современные облачные вычисления могут обеспечить высокий уровень защиты хранимых данных, однако уязвимости системы могут привести к несанкционированному доступу и повлечь за собой потерю целостности, и конфиденциальности информации. Поэтому решение проблемы обеспечения должного уровня безопасности является одной из первостепенных задач при работе с облачными сервисами. По прогнозу Stratview (Cloud Security Market), объем мирового рынка облачной безопасности в период с 2022 до 2028 года вырастет с 46,36 до 100,96 млрд долларов при среднегодовом показателе роста 13,85%. (Рисунок 1.) [2]

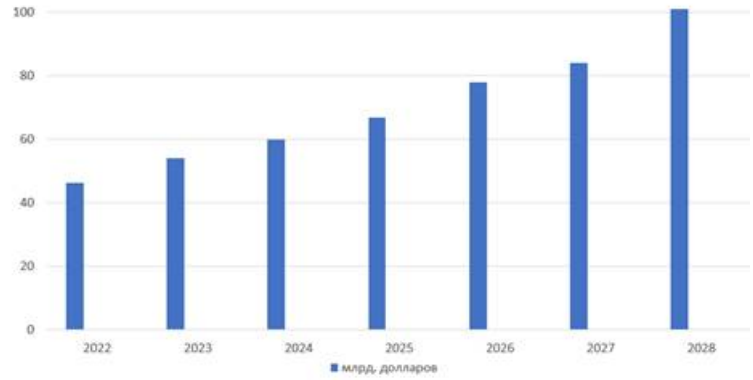

Рисунок 1. Прогноз объема мирового рынка облачной безопасности в период с 2022г. до 2028г.

Информационная безопасность в облаке должна основываться на обеспечение основных принципов информационной безопасности: конфиденциальность, целостность и доступность информации или средств ее обработки.

Нормативно-правовые акты, регулирующие работу облачных хранилищ

Выделим ряд нормативно-правовых актов, которые регулируют работу в сфере облачных технологий:

1. ГОСТ Р ИСО/МЭК 17826-2015 «Информационные технологии. Интерфейс управления облачными данными (CDMI)».

2. ГОСТ Р 56938-2016 «Защита информации. Защита информации при использовании технологий виртуализации. Общие положения». Стандарт определяющий требования по защите информации, обрабатываемой с использованием технологий виртуализации.

3. ГОСТ ISO/IEC 17788-2016 «Межгосударственный стандарт. Информационные технологии облачные вычисления. Общие положения и терминология Information technology. Cloud computing. Overview and vocabulary».

4. 149-ФЗ «Об информации, информационных технологиях и о защите информации».

5. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ. В соответствии с Федеральным законом запись, систематизация, накопление, хранение, обновление, изменение или извлечение персональных данных должны производиться на сервере, который физически расположен на территории Российской Федерации. Необходимо учитывать, что облачному провайдеру не предоставляется доступ к информационным системам, которые размещены в облаке, соответственно, ответственность по обеспечению безопасности персональных данных возлагается на оператора.

6. Постановление Правительства РФ № 1119 регламентирует разработку системы защиты персональных данных.

7. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Документ определяет требования по мерам обеспечения безопасности персональных данных, направленных на нейтрализацию актуальных угроз безопасности персональных данных. Состав и содержание мер по обеспечению безопасности персональных данных

определяется в соответствии с определенным уровнем защищенности персональных данных. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Документ направлен на формирование требований к защите информации, содержащейся в государственных информационных системах.

Специфика безопасности облачных хранилищ

По результатам отчета по безопасности облачных вычислений в 2022 г. (Cloud Security Report 2022), основанном на всестороннем глобальном исследовании кибербезопасности мирового сообщества:

· Большинство организаций продолжают использовать гибридную (39 % по сравнению с 36 % в прошлом году) или многооблачную стратегию. (33%) для интеграции нескольких сервисов в целях масштабируемости или обеспечения непрерывности бизнеса. (76%) используют двух или более облачных провайдеров.

· Организации продолжают быстро перемещать рабочие нагрузки в облако. Сегодня 39% опрошенных имеют более половины своих рабочих нагрузок в облаке, а 58% планируют выйти на этот уровень в ближайший год.

· Пользователи облака подтверждают, что облако обеспечивает гибкую емкость и масштабируемость (53%), а также способствуют повышению доступности и непрерывности бизнеса (45%). [3]

Безопасность в облаке по-прежнему вызывает серьезную озабоченность у специалистов по кибербезопасности. Порядка 95% респондентов обеспокоены состоянием своей безопасности в общедоступной облачной среде. Безопасность облака за счет своей специфики отличается от традиционных подходов к безопасности информационных технологий. Рассмотрим основные аспекты:

· Данные при хранении в облаке находятся на общедоступных серверах, что повышает риск несанкционированного доступа к данным, при этом ответственность за безопасность информации лежит на организации-потребителе, а не на поставщике услуг. При этом, не каждая организация располагает средствами для проведения аудита безопасности и другими средствами контроля безопасности системы. Несбалансированность системы безопасности может кардинально сказаться на качестве работы с данными в облачном решении. [4]

· Использование в облаке модульной инфраструктуры облегчает адаптацию системы, однако взаимодействие виртуальных машин (клонирование, изменение масштабируемости, перемещение между серверами) в облаке может привести к нарушению целостности системы безопасности. Решением данной проблемы является шифрование данных, которое требует увеличение количества ресурсов, что сказывается на быстродействии системы, однако значительно повышает безопасность. При этом необходим индивидуальный подход к определению параметров настройки системы, который может меняться на основании частоты использования виртуальной машины и статуса информации, подвергающейся хранению и обработке. Уязвимости системы находятся вне всякого контроля во время распространения и, следовательно, могут возникать через неограниченное время. Поэтому очень важно постоянно контролировать

состояние защиты системы, независимо от ее местоположения. [5]

· Проблему уязвимости виртуальных машин к заражению вредоносным программным обеспечением позволяют решить системы обнаружения и предотвращения вторжений. При этом важно помнить, что статус виртуальной машины (активна/неактивна) не влияет на возможность заражения вирусами. Решением этой проблемы может стать подключение хранилища образов виртуальной машины к сети, в случае неактивности виртуальной машины требуются дополнительные меры защиты. [6]

· Охват сети не стабилен и не имеет четких границ, а в некоторых случаях исчезает полностью. Виртуальные машины должны обеспечивать собственную защиту, перемещая периметр сети непосредственно на саму виртуальную машину, разделяя тем самым части системы с разным уровнем доверия в облаке.

· Облачные системы взаимодействуют со многими другими системами и службами, которые должны быть защищены как на уровне организаций, так и для физических лиц. Права доступа должны управляться на всех уровнях. Поставщики и пользователи должны отслеживать уязвимости, вызванные небезопасной установкой приложений и доступом к системе. [7]

· Работа исключительно через Интернет приводит к невозможности контроля доступа на физическом уровне и как следствие – необходимость формирования политики разграничения доступа пользователей по ролям с обеспечением прозрачности действий.

· Поставщик облачных услуг и клиент не всегда работают в коллаборации, разделяя между собой ответственность по обеспечению высокого уровня безопасности облачного хранилища. [8]

Лучшим решением построения облачной системы с высоким уровнем безопасности является концепция построения многоуровневой безопасности. Такой подход позволит не только увеличить временные затраты, но и трудоемкость процесса проникновения злоумышленника в систему. Это повысит шансы своевременного распознавания и предотвращения различного типа атак.

Необходимо учитывать, что информационная безопасность усложняется для более распределенной инфраструктуры. Это связано с большим количеством хостов и сервисов, увеличивающих зону действия злоумышленников.

В качестве решения можно предложить следующий набор действий:

· **Шифрование.** Выбор надежного метода шифрования гарантирует большое количество вычислительных и временных ресурсов для злоумышленника в процессе дешифрования. Шифрование и расшифрование происходит по ключу, как правило, в режиме блочного шифрования. Алгоритм шифрования является встроенным и зависит от выбора системы (например, система LUKS используемая в ОС на основе ядра Linux, использует AES подобный блочный шифр с размером ключа 256 бит). Настройки шифрования производятся индивидуально для всех частей системы. Надежность шифрования будет зависеть не только от параметров настройки и выбора алгоритма, но и от политики хранения ключей и невозможности их компрометирования.

· **Выбор надежного метода аутентификации**. Например, гиперконвергентная платформа облачных вычислений для создания и управления частными, гибридными и общедоступными облаками и центрами обработки данных OpenNebula использует

двухфакторную аутентификацию, разграничивая и отслеживая используемые ресурсы для отдельных групп пользователей.

· **Использование межсетевого экрана**, с целью фильтрации трафика и предотвращения вторжений. Удобно использовать файрволы встроенные в ядро операционной системы (например, NetFilter или ConfigServer Security Firewall для Linux). При написании правил эффективнее использовать подход: «что не разрешено, то запрещено».

· **Обеспечение передачи данных по сети интернет в защищенном исполнении.** (Причиной является расположение серверов за пределами корпоративной сети компании).

· **Использование системы обнаружения и предотвращения вторжений.** (Например, IPS/IDS система Suricata, позволяющая не только детектировать атаки и блокировать подозрительные интеграции, но и обрабатывать пакеты, меняя маршруты на основании их содержания.

Особенности работы с облачными вычислениями формируют политику безопасности в области облачных сервисов. Рост угроз безопасности в сфере облачных технологий требует индивидуальный и комплексный подход к решению данной проблемы. Анализ специфики угрозы информационной безопасности облачных систем позволяет сделать выводы о необходимости формирования многоуровневой комплексной защиты, включающей в себя шифрование, аутентификацию, использование межсетевых экранов, антивирусной защиты и др. Грамотная политика по обеспечению безопасности в сфере облачных решений позволит увеличить объемы и перспективы их использования.

Библиография

1. Клементьев И. П., Устинов В. А. Введение в Облачные вычисления: ИНТУИТ, 2016.
2. Toutov A. et al. Optimizing the Migration of Virtual Machines in Cloud Data Centers // International Journal of Embedded and Real-Time Communication Systems (IJERTCS). 2022. Vol. 13. No. 1. Pp. 1-19.
3. Миронова А. О. и др. Применение методики оценки угроз безопасности информации // Энергетические установки и технологии. 2021. Т. 7. №. 4. С. 71.
4. Акбарова М. Р. Безопасность и защита данных в облачных технологиях // Universum: технические науки. 2022. №. 10-1 (103). С. 17-19.
5. Нестеренко В. Р., Маслова М. А. Современные вызовы и угрозы информационной безопасности публичных облачных решений и способы работы с ними // Научный результат. Информационные технологии. 2021. Т. 6. №. 1. С. 48-54.
6. Alshamrani A. et al. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities // IEEE Communications Surveys & Tutorials. 2019. Vol. 21. No. 2. Pp. 1851-1877.
7. Canizo M. et al. Multi-head CNN–RNN for multi-time series anomaly detection: An industrial case study // Neurocomputing. 2019. Vol. 363. Pp. 246-260.
8. Ahmed M., Mahmood A. N., Hu J. A survey of network anomaly detection techniques // Journal of Network and Computer Applications. 2016. Vol. 60. Pp. 19-31.

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.

Со списком рецензентов издательства можно ознакомиться здесь.

Предметом рецензируемого исследования выступает крайне актуальная в современном информационном мире проблема безопасности облачных систем хранения данных. Учитывая отмечаемый многими экспертами (например, Базальт СПО, Positive Technologies, ИБ-центр ФСБ и др.) факт ежегодного роста на десятки процентов (например, только за 2022-й год рост составил 21 %) кибератак на информационную инфраструктуру России, весьма высокой следует признать и прикладную значимость рецензируемой статьи. К сожалению, автор не дал себе труда хоть как-то отрефлексировать используемую методологию. Но из контекста можно понять, что кроме традиционных общенаучных аналитических методов использовались нормативно-институциональный (при анализе нормативно-правовой базы, регулирующей работу облачных хранилищ в России), статистический анализ вторичных социологических данных (при выявлении специфики безопасности облачных хранилищ в России), а также некоторые методы анализа рисков информационной безопасности. Вполне корректное применение перечисленных методов позволило автору получить результаты, обладающие некоторыми признаками научной новизны. Прежде всего, речь идёт о выявленной и адаптированной для социально-гуманитарного знания специфике обеспечения безопасности облачных систем хранения данных в России, с акцентом на их нормативном и технологическом аспектах. В этом контексте вполне полезным представляется развиваемый автором применительно к облачным хранилищам концепт многоуровневой безопасности. Наконец, определённый интерес представляют сформулированные автором конкретные рекомендации по решению проблем информационной безопасности облачных систем хранения данных. В структурном плане работу также следует признать вполне продуманной: её логика последовательна и отражает основные аспекты проведённого исследования. В тексте выделены следующие разделы: - неозаглавленная вводная часть, где ставится научная проблема и обосновывается её актуальность, но к сожалению, отсутствует постановка целей и задач, а также теоретико-методологическая рефлексия; - «Нормативно-правовые акты, регулирующие работу облачных хранилищ», где анализируется юридическая база функционирования облачных систем хранения данных в России, но к сожалению, отсутствует сравнение российской нормативной базы с таковой в других странах; - «Специфика безопасности облачных хранилищ», где исследованы особенности обеспечения безопасности хранения данных в «облаках», а также обоснована необходимость применения концепции многоуровневой безопасности; - неозаглавленная заключительная часть, где подводятся итоги проведённого исследования и формулируются конкретные рекомендации по обеспечению безопасности хранения данных в облачных системах. С точки зрения стиля рецензируемая статья также не вызывает серьёзных нареканий: стиль текста соответствует основным критериям научности, а также литературным и языковым нормам. Хотя в тексте встречается некоторое количество стилистических (например, не очень удачные с точки зрения стиля формулировки «Выбор надежного метода шифрования гарантирует большое количество вычислительных и временных ресурсов для злоумышленника в процессе дешифрования» и др.) и грамматических (например, несогласованное предложение «Информационная безопасность в облаке должна основываться на обеспечениЕ основных принципов информационной безопасности…»; или некорректное начало предложений со скобок с цифрами, например: «(33%) для интеграции нескольких сервисов в целях масштабируемости…»; и др.) погрешностей, но в целом он написан достаточно грамотно, на хорошем русском языке, с корректным использованием научной терминологии. Библиография насчитывает 8 наименований, в

том числе источники на иностранных языках, и в должной мере репрезентирует состояние исследований по проблематике статьи. Апелляция к оппонентам имеет место при обсуждении специфики безопасности облачных хранилищ данных.

ОБЩИЙ ВЫВОД: предложенную к рецензированию статью можно квалифицировать в качестве научной работы, соответствующей основным требованиям, предъявляемым к работам подобного рода. Несмотря на некоторые огрехи (которые, как надеется рецензент, будут устранены автором в его будущих работах), результаты проведённого исследования будут представлять интерес для политологов, социологов, специалистов в области информационной безопасности, а также для студентов перечисленных специальностей. Небезынтересными эти результаты могут оказаться и для представителей российского бизнеса. Представленный материал соответствует тематике журнала «Вопросы безопасности». По результатам рецензирования статья рекомендуется к публикации.