

ОБЛАЧНЫЕ ТЕХНОЛОГИИ В ПРОЦЕССЕ АУДИТА И КОНТРОЛЯ ЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Т.В. Денисова¹, levkutnaiatv@susu.ru

А.Г. Терновская², aleksandra15022003@yandex.ru

¹ Южно-Уральский государственный университет, Челябинск, Россия

² ООО «Авантаж», Челябинск, Россия

Аннотация. В статье рассматриваются преимущества использования облачных технологий в аудиторской деятельности. Аудит позволяет контролировать финансовые потоки, выявлять и устранять нарушения и недочеты в управлении ресурсами, обеспечивать прозрачность и достоверность финансовой отчетности. В связи с потребностью обработки большого массива данных, глобальной тенденции к сокращению времени на сбор информации, проверки и анализа, а также с актуальностью быстрого доступа к оперативной информации, в аудиторской деятельности все более востребованными становятся облачные технологии, которые облегчают и ускоряют производственные и управленческие процессы. Одним из главных преимуществ облачных технологий является возможность использования и доступа к данным из любой точки мира, с любого устройства, без необходимости физического присутствия на месте. Посредством проведения обзора информации и ее анализа были выявлены преимущества и ограничения использования облачных технологий в деятельности аудитора.

Ключевые слова: аудит, облачные технологии, контроль, защита данных

Для цитирования: Денисова Т.В., Терновская А.Г. Облачные технологии в процессе аудита и контроля за информационной безопасностью // Вестник ЮУрГУ. Серия «Экономика и менеджмент». 2024. Т. 18, № 2. С. 191–194. DOI: 10.14529/em240217

Brief report
DOI: 10.14529/em240217

CLOUD TECHNOLOGIES IN THE PROCESS OF AUDIT AND CONTROL OVER INFORMATION SECURITY

T. V. Denisova¹, levkutnaiatv@susu.ru

A. G. Ternovskaya², aleksandra15022003@yandex.ru

¹ South Ural State University, Chelyabinsk, Russia

² Avantazh LLC, Chelyabinsk, Russia

Abstract. This article discusses the advantages of using cloud technologies in audit activities. The audit allows you to control financial flows, identify and eliminate violations and shortcomings in resource management, and ensure transparency and reliability of financial statements. In connection with the need to process a large array of data, a global tendency to reduce time to collect information, verification and analysis, as well as with the relevance of quick access to operational information, cloud technologies are increasingly popular in audit activities that facilitate and accelerate production and managerial processes. One of the main advantages of cloud technologies is the ability to use and access data from anywhere in the world, from any device, without the need for physical presence on the spot. Through the review of information and its analysis, the advantages and restrictions of the use of cloud technologies in the activities of the auditor were identified.

Keywords: audit, cloud technologies, control, data protection

For citation: Denisova T.V., Ternovskaya A.G. Cloud technologies in the process of audit and control over information security. *Bulletin of the South Ural State University. Ser. Economics and Management*, 2024, vol. 18, no. 2, pp. 191–194. (In Russ.). DOI: 10.14529/em240217

Аудит является процессом независимой проверки финансовой деятельности организации с целью подтверждения достоверности и надежности ее финансовой отчетности. Аудиторы проводят комплексный анализ финансовых данных, оценивают эффективность системы управления и контроля, выявляют возможные нарушения и рекомендуют меры по их устранению. Аудиторская проверка обеспечивает доверие к финансовой отчетности организации со стороны партнеров и клиентов, что в свою очередь способствует притоку инвестиций, повышению репутации компании на рынке.

Облачные технологии – это способ предоставления информационных, вычислительных и других ресурсов через удаленные центры обработки данных (облако), доступ к которым осуществляется через интернет. Облачные технологии позволяют пользователям получать доступ к данным и работать с ними из любой точки мира, обеспечивают гибкость, масштабируемость и экономичность. Проще говоря, облако – это виртуальная инфраструктура, которая позволяет использовать вычислительные мощности, программное обеспечение, хранилища без необходимости физического владения или управления ими. Такой подход освобождает пользователей от необходимости приобретать и обслуживать собственные серверы и дата-центры, повышает эффективность производства, управления финансовой деятельностью. Облачные сервисы можно арендовать у провайдеров, например, Dropbox, iCloud, Google Диск и SkyDrive за ежемесячную или годовую плату [1].

Облачные технологии в современных условиях активно используются в аудиторской практике, формировании отчетности для повышения эффективности и надежности деятельности организации. Авторы систематизировали направления улучшений, привносимые облачными технологиями:

1. Хранение данных. Облачные хранилища обеспечивают безопасное хранение документов, необходимых для проведения аудита. В то же время это предполагает применение способов достижения безопасности хранения через шифрование, управление доступом и регулярное резервирование при соблюдении нормативных требований при обработке и хранении конфиденциальной информации [2].

2. Одновременный многопользовательский доступ. Облачные платформы совместной работы позволяют участникам аудита работать над документами и отчетами одновременно, обмениваться информацией, что при прочих равных условиях повышает коммуникацию и сотрудничество между членами команды.

3. Мониторинг и аналитика. Облачные сервисы аналитики данных позволяют быстро и эффективно анализировать большие объемы информации, выявлять проблемы, что повышает качество

аудита. Облачные платформы позволяют автоматизировать сбор данных, анализировать финансовые отчеты, проверять финансовые транзакции и даже использовать специализированные аудиторские инструменты для обнаружения аномалий или подозрительной деятельности. Анализ больших объемов данных, предоставляемый облачными технологиями, также позволяет выявлять тенденции, прогнозировать возможные риски или потенциальные области несоответствия.

4. Автоматизация процессов. Облачные платформы автоматизации процессов позволяют упростить и ускорить выполнение задач аудитора, например, сбор информации, анализ данных и формирование отчетности. Появляется простой способ предоставления корпоративных порталов с различными возможностями, такими как графики календарного планирования, графики отсутствия, интегрированные системы взаимодействия с клиентами, план текущих задач, доступ к отчетности и т. д. [3].

5. Использование и анализ аудиофайлов в аудите с помощью специализированных облачных сервисов (например, распознавание речи, фильтрация шумов и т. д.).

6. Безопасность и конфиденциальность. Многие облачные провайдеры обладают высокими стандартами безопасности и шифрования данных, что обеспечивает защиту конфиденциальности информации и предотвращает утечку данных.

Что касается контроля за информационной безопасностью, облачные технологии также играют ключевую роль, с их помощью возможно создать надежные системы защиты данных, предотвращать утечки информации, идентифицировать угрозы на ранних этапах.

Безусловно, защита конфиденциальной информации является первостепенной задачей для организаций, которые хранят клиентские данные или финансовую информацию. Это включает в себя реализацию мер по обнаружению и предотвращению любых форм несанкционированного доступа как непреднамеренного, так и злонамеренного. Согласно недавнему исследованию Ponemon Institute, стоимость инсайдерских угроз значительно возросла. В период с 2019 по 2021 год ущерб от таких инцидентов увеличился на 31 %, достигнув 11,45 миллиона долларов. Более того, частота инсайдерских угроз также возросла на 47 % за тот же период. В отчете Ponemon Institute за 2019 год отмечается, что основные опасения организаций связаны с непреднамеренными нарушениями инсайдеров – около 71 %, утечками данных из-за халатности – 65 % – и злонамеренными атаками – 60 % [4]. Это подчеркивает необходимость комплексного подхода к защите данных, учитывающего как внутренние, так и внешние угрозы.

Защита данных – это необходимость, требующая определенных финансовых затрат, но в

настоящее время есть множество способов избежать нежелательной утечки информации:

1. Шифрование данных перед их передачей в облако и во время хранения, что поможет защитить информацию от несанкционированного доступа при пересылке и хранении. Компания может зашифровать свои данные независимо самостоятельно, прежде чем поместить их в облако, либо воспользоваться услугами облачного провайдера, который зашифрует данные в рамках предоставляемых услуг. Однако, если у компании хранятся только не конфиденциальные данные в облаке, например, корпоративная графика или видео, то сквозное шифрование может быть избыточным. Но, с другой стороны, для финансовых, конфиденциальных или коммерческих данных это может быть критически важным [5].

2. Двухступенчатая (многофакторная) аутентификация как метод проверки подлинности, который использует два или более различных факторов для подтверждения личности пользователя.

3. Регулярное обновление паролей, практики регулярной смены ключей шифрования.

4. Ограничение доступа (Identity and access management, IAM) через управление правами доступа к информации в облаке, то есть наделение только теми правами сотрудников, которые им необходимы для выполнения рабочих задач.

5. Резервное копирование данных, чтобы обеспечить их сохранность в случае сбоя системы или кибератаки. Это позволяет применить меры аварийного восстановления в случае потери данных.

6. Мониторинг и аудит активности в облаке и проведение регулярных аудитов безопасности для выявления потенциальных угроз и нарушений, предотвращения вторжений (IPS) [6], применение системы управления информационной безопасностью (ISMS). IPS анализирует сетевой трафик и выявляет подозрительную активность, предотвращая в режиме реального времени атаки и несанкционированный доступ [7, 8].

Без доступа к интернету использование облачных технологий становится невозможным, так как пользователи не смогут получить доступ к своим данным, работать с приложениями и серви-

сами, а также не смогут обмениваться информацией с другими пользователями. Сама компания, которую проверяет аудитор, должна иметь постоянный доступ к интернету, чтобы вовремя вносить и изменять цифровые документы, либо в короткое время вносить данные в систему после восстановления доступа к интернету. Также и аудитор должен иметь доступ к сети, чтобы иметь возможность проверить необходимую документацию. Либо же пользователи должны иметь локальное подключение.

Защита конфиденциальных данных требует многоуровневого подхода, который рассматривает как внутренние, так и внешние угрозы. Реализация изложенных выше мер и постоянное отслеживание рисков безопасности позволяют организациям снизить вероятность инсайдерских угроз и утечек данных, защищая конфиденциальность клиентов, сотрудников и организации в целом. При этом пользователи должны обеспечить себе надежное подключение к сети для эффективной работы с облачными сервисами.

Внедрение облачных технологий в аудиторскую практику позволяет компаниям быть конкурентоспособными и обеспечивает им надежность и защиту в цифровой эпохе. Особенно данные технологии помогут аудитору быстро получать данные от проверяемого предприятия, сократится необходимость личного присутствия аудитора у аудируемого предприятия, сократится общее время проверки.

Эти невидные упрощения процессов в условиях устойчивого развития экономики очень важны для финансового контроля и аудита, поскольку сокращают затрачиваемое время и ресурсы, способствуют повышению прозрачности и ответственности в управлении ресурсами, предотвращают финансовые махинации, уклонение от уплаты налогов и другие негативные явления. Они также помогают снижать риски финансовых потерь, обеспечивать эффективное распределение ресурсов и содействуют устойчивому экономическому росту.

Таким образом, внедрение облачных технологий в аудиторскую деятельность помогает улучшить качество оказываемых услуг и снизить их стоимость.

Список литературы

1. Что такое облачные технологии и как они работают. URL: <https://journal.sovcombank.ru/tehnologii/chto-takoe-oblachnie-tehnologii-i-kak-oni-rabotayut>
2. Облачное хранилище. URL: <https://blog.skillfactory.ru/glossary/oblachnoe-hranilishe/>
3. Смирнов Н.А. Облачные технологии в автоматизации деятельности организации // Евразийский Союз Ученых. 2016. № 4-1 (25). URL: <https://cyberleninka.ru/article/n/oblachnye-tehnologii-v-avtomatizatsii-deyatelnosti-organizatsii>.
4. Аудит в CDP Private Cloud Base с использованием внешних систем. URL: <https://habr.com/ru/companies/cloudera/articles/571536/>
5. Подходы к аудиту информационной безопасности систем облачных вычислений (cloud security). URL: <https://www.audit-it.ru/articles/soft/a118/1081024.html#sdfootnote1sym>

6. IPS/IDS – системы обнаружения и предотвращения вторжений. URL: <https://selectel.ru/blog/ips-and-ids/>
7. What is an ISMS (Information Security Management System)? URL: <https://www.upguard.com/blog/isms>
8. Атаки нулевого дня, APT-атаки и защита от них с использованием решений Check Point. URL: <https://habr.com/ru/companies/muk/articles/220657/>

References

1. *Что такое облачные технологии и как они работают* [What are cloud technologies and how do they work]. URL: <https://journal.sovcombank.ru/tehnologii/что-такое-облачные-технологии-и-как-они-работают>
2. *Облачное хранилище* [Cloud storage]. URL: <https://blog.skillfactory.ru/glossary/oblastnoe-hranilishe/>
3. Smirnov N.A. Cloud technologies in automating the activities of an organization. *Evraziyskiy Soyuz Uchenykh* [Eurasian Union of Scientists], 2016, no. 4-1 (25). (In Russ.) URL: <https://cyberleninka.ru/article/n/oblastnye-tehnologii-v-avtomatizatsii-deyatelnosti-organizatsii>.
4. *Audit v CDP Private Cloud Base s ispol'zovaniem vneshnikh sistem* [Audit in CDP Private Cloud Base using external systems]. URL: <https://habr.com/ru/companies/cloudera/articles/571536/>
5. *Podkhody k auditu informatsionnoy bezopasnosti sistem oblastnykh vychisleniy (cloud security)* [Approaches to auditing information security of cloud computing systems (cloud security)]. URL: <https://www.audit-it.ru/articles/soft/a118/1081024.html#sdfootnote1sym>
6. *IPS/IDS – системы обнаружения и предотвращения вторжений* [IPS/IDS – intrusion detection and prevention systems]. URL: <https://selectel.ru/blog/ips-and-ids/>
7. *What is an ISMS (Information Security Management System)?* URL: <https://www.upguard.com/blog/isms>
8. *Ataki nulevogo dnya, APT-ataki i zashchita ot nikh s ispol'zovaniem resheniy Check Point* [Zero-day attacks, APT attacks and protection against them using Check Point solutions]. URL: <https://habr.com/ru/companies/muk/articles/220657/>

Информация об авторах

Денисова Тая Виталиевна, к.э.н., доцент кафедры экономики и финансов, Южно-Уральский государственный университет, Челябинск, Россия; levkutnaiatv@susu.ru

Терновская Александра Георгиевна, ассистент аудитора, ООО «Авантаж», Челябинск, Россия; aleksandra15022003@yandex.ru

Information about the authors

Taya V. Denisova, Ph.D., Associate Professor, Department of Economics and Finance, South Ural State University, Chelyabinsk, Russia; levkutnaiatv@susu.ru

Alexandra G. Ternovskaya, assistant auditor, Avantazh LLC, Chelyabinsk, Russia; aleksandra15022003@yandex.ru

Статья поступила в редакцию 21.06.2024

The article was submitted 21.06.2024