Формирование информационно-образовательной среды

УДК 37.02

О.Ю. Заславская,
А.В. Иванов

Проблемы безопасности при использовании облачных технологий в образовательных организациях

В статье обсуждается использование облачных технологий в деятельности образовательной организации, анализируются возможные риски в области безопасности при использования облачных технологий в образовательных организациях.

Ключевые слова: облачные технологии; управление образованием; безопасность; информационные технологии в образовании; информационно-образовательная среда.

Облачные технологии играют важную роль в развитии управления образовательной организацией, а также качеством образования, обеспечивая достижение необходимого уровня образовательного процесса [10]. Облачные технологии позволяют пользователям хранить важную информацию на сервере с обеспечением повсеместного доступа к ней. Службы и приложения, реализованные на основе облачных технологий, дают возможность пользователям хранить и получать доступ к своим локальным данным, размещенным в удаленном центре обработки данных, и использовать для работы как персональные компьютеры, так и мобильные устройства[1]. В образовательных организациях облачные технологии способны обеспечить всем участникам процесса обучения, включая обучающихся, преподавателей, родителей, сотрудников школы, администрацию и даже дополнительный персонал, доступ к образовательным технологиям [4; 9].

Образовательные сервисы, реализованные на основе облачных технологий, имеют пять основных функциональных направлений: возможность самостоятельной работы пользователя, повсеместный доступ (если есть сеть Интернет),

[1] *Mell P., Grance T.* The NIST Definition of Cloud Computing. NIST, USA. 2011. URL: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpu blication800-145.pdf (дата обращения: 16.11.2017).

© Заславская О.Ю., Иванов А.В., 2018

объединение ресурсов, возможность быстрого изменения данных, использование внутренней статистики о работе облачных служб [1]. Рассмотрим особенности выделенных направлений с точки зрения обеспечения безопасности используемых в процессе обучения данных.

Пользователям в образовательных организациях требуется выполнение различных функций и операций. При этом желательно обеспечить им определенную свободу действий для выбора и использования тех или иных облачных сервисов или ресурсов из всего многообразия облачных технологий. Как правило, пользователь облачных сервисов сам настраивает и управляет всеми ресурсами, к которым имеет доступ, или запрашивает этот доступ на право использования необходимых технологий через веб-интерфейс у администратора образовательной среды. Такой перечень доступов может быть очень обширен: от самостоятельного сброса или изменения пароля своей учетной записи (без необходимости обращаться к преподавателю или административному работнику) до доступа к учебным материалам или управленческим отчетам, в том числе интерактивным.

Повсеместный доступ основан на том, что облачные технологии сегодня широко доступны с любых устройств, имеющих самые различные операционные системы (ноутбуки, планшеты, мобильные телефоны и т. д.), и отовсюду (как из сети образовательной организации, так и из дома, библиотеки или др.). Повсеместный доступ основан на применении стандартных механизмов и протоколов передачи данных. Подключение такого уровня доступа разным категориям пользователей образовательной организации требует, чтобы образовательные облачные технологии были адаптированы согласно запросам этих пользователей.

Объединение ресурсов основано на том, что для обслуживания нескольких пользователей используется один набор из множества ресурсов. Эта многопользовательская модель основывается на технологиях виртуализации, в которой ресурсы динамически назначаются и повторно используются согласно требованию пользователей. Многопользовательская облачная среда характеризуется тем, что пользователь ничего не знает о том, где в настоящее время расположены или хранятся его данные.

Возможность быстрого изменения ресурсов основана на учете политик безопасности и реализуется за счет установленных прав. Например, масштабирование заранее подготовленных сервисов происходит на основе политик и требований к пользователям или к их устройствам. Так, например, можно запретить доступ к ресурсам образовательной организации с устройств, на которых не установлено и не обновлено антивирусное программное обеспечение. Какие-либо изменения ресурсов не оказывают влияния на приложения, размещенные в облаке, и не требуют постоянного человеческого участия для их корректировки. Различные заинтересованные стороны в образовательной организации, такие как обучающиеся, преподаватели, административный персонал

и другие, могут получить доступ и использовать образовательные ресурсы при необходимости, а требуемые вычислительные и мультимедийные мощности выделяются на основе политик доступа и безопасности автоматически, в любое время.

Использование внутренней статистики и отчетности позволяет организовать систему контроля и учета использования образовательных облачных технологий [13]. Она обычно включает различные счетчики, в том числе ресурсы, используемые в образовательном процессе, формы сбора отчетов о производительности. Отчеты об использовании образовательных облачных технологий или ресурсов обеспечивают прозрачность статистики как для пользователя, так и для руководителя образовательной организации, организации обеспечивающей предоставление доступа к облачным технологиям, а также могут предоставить дополнительные показатели, необходимые для принятия решений при управлении образовательным процессом. При этом использование образовательных облачных технологий экономически более эффективно по сравнению с использованием локальных программных и аппаратных средств инфраструктуры.

Имеются три основные группы облачных технологий, которые пользователь может получить в образовательной организации: программное обеспечение как услуга (далее — SaaS (от *англ.* Software as a Service)), платформа как сервис (далее — PaaS (от *англ.* Platform as a Service)) и инфраструктура как услуга (далее — IaaS (от *англ.* Infrastructure as a Service)) [15]. Но эти группы используют друг друга, из чего следует, что необходимо рассматривать все эти группы при формировании системы безопасности, даже если в данный момент используется только одна.

В модели SaaS (модель использования бизнес-приложений в формате интернет-сервисов) пользователи получают доступ к опубликованным приложениям в любое время. В настоящее время SaaS считается наиболее широко востребованным видом облачных технологий в сфере образования. Диски Yandex и Google, сервисы Twitter, «ВКонтакте», Dropbox, YouTube и OneDrive, набор приложений Office 365 — наиболее яркие примеры SaaS. Компании Microsoft и Google предоставляют некоторые услуги, специально созданные для образования и образовательных учреждений, все они основаны на модели SaaS [12].

В PaaS (облачная среда, которую можно использовать для разработки, тестирования и запуска приложений, а также для управления ими) поставщик технологий предоставляет разработчикам средства разработки для создания или настройки их приложения или службы в облаке, независимо от платформы для запуска. Известным примером PaaS является Google App Engine, где разработчик может установить и настроить работу приложения с помощью языка Python.

IaaS (вычислительная инфраструктура (серверы, хранилища данных, сети, операционные системы), которая предоставляется пользователям для разворачивания

и запуска собственных программных решений) — это доступ к вычислительным ресурсам, которые можно удаленно контролировать (процессоры, место для хранения, виртуальные сети и т. д.) в центре данных и использовать их для запуска собственных операционных систем и приложений. Большим преимуществом использования IaaS является то, что она предлагает свой центр данных по требованию без необходимости покупки или установки нового дорогостоящего оборудования. Microsoft Azure и Amazon Elastic Compute Cloud являются самыми распространенными примерами IaaS.

Проблемы безопасности данных связаны главным образом с тремя основными требованиями: обеспечение конфиденциальности и целостности данных и их доступности. Конфиденциальность определяется как набор правил, которые предотвращают несанкционированный доступ к хранимой информации, целостность же понимается как способ защиты данных от их несанкционированного изменения и как подтверждение, что данные извлекаются без случайных или преднамеренных искажений и являются достоверными. Соблюдение требования доступности позволяет авторизованным пользователям получать надежный доступ к данным, что особенно важно, если они находятся вне пределов образовательной организации.

Чтобы понять и успешно решать вопросы безопасности данных, размещенных в облаке, и уметь грамотно оценить проблемы их безопасности в образовательных организациях, необходимо рассмотреть различные аспекты использования облачных технологий, особенно возможные угрозы и риски при информационных атаках [7].

Безопасность среды передачи информации, с помощью которой пользователь подключается к облачной инфраструктуре, является важным направлением защиты. Обеспечение безопасности такой среды предотвращает потерю конфиденциальной информации во время ее передачи [3].

Наибольшие проблемы безопасности связаны с сетью передачи данных, так как все операции при использовании облачных технологий полностью зависят от нее, а все пользователи используют свои данные в режиме удаленного доступа.

Безопасность облачной инфраструктуры ставит вопросы, связанные с работой физического оборудования, используемого в качестве основы для облачной инфраструктуры, а также со средствами виртуализации, используемыми для работы облачных ресурсов.

Одной из задач обеспечения безопасности виртуальной среды является защита виртуальной машины, потому что когда несколько виртуальных машин расположены на одном компьютере, вы не можете поставить аппаратное устройство защиты, например брандмауэр, между ними. Еще одна проблема обусловлена динамичной средой, в которой виртуальные машины создаются, удаляются или переносятся в другое расположение автоматически, что затрудняет контроль этого движения и определение факта нарушения безопасности.

Можно сформулировать следующие рекомендации по безопасному использованию облачных технологий:

1. Облачные технологии дают очень много преимуществ, но от администраторов, обслуживающих серверы, и от административно-управленческого персонала требуется понимание принципов работы облачных технологий и строгое следование рекомендациям и стандартам обеспечения безопасности информации, а также знание и выполнение законов и подзаконных актов по работе с персональными данными.

2. Сети и среды передачи информации в образовательной организации должны быть готовы для облачных технологий. Это означает, что сетевое оборудование (маршрутизаторы, брандмауэры и т. п.) должно быть настроено так, чтобы доступ в облако был наиболее безопасным и достигались ожидаемые результаты от использования облачных технологий. Кроме того, нужно рассмотреть вопросы возможности изоляции сети (например, на основе протоколов VPN, VLAN, и т. д.).

3. Выделенный ИТ-администратор должен постоянно контролировать и управлять облачными услугами, что протоколируется при заключении договора с поставщиком технологий.

4. Рекомендуется заключить договор с третьей стороной с целью проведения проверок на регулярной основе для мониторинга производительности и соответствия предоставляемых услуг с согласованными по договору с поставщиком условиями. Аудит ИТ позволит вовремя выявить проблемы в области безопасности (и не только здесь) при использовании облачных технологий.

5. Периодически необходимо контролировать производительность имеющихся облачных технологий и вносить изменения. Эта процедура может уменьшить угрозы безопасности и снизить риски в работе.

6. Применение стратегии оценок угроз является настоятельной необходимостью. В зависимости от категории обрабатываемой информации это также может стать требованием по выполнению законов о защите персональных данных. Иногда заинтересованные стороны просто не были осведомлены о конкретных угрозах в облачной инфраструктуре. Это требует нахождения надежных способов обнаружения угроз, что позволит избежать даже их возникновение. Подобные меры должны быть приняты специально для устранения потенциальных внутренних угроз.

7. Данные и приложения в облачной среде должны классифицироваться на основе их значений согласно их важности и чувствительности к модификации и доступу. Не все данные, хранящиеся в облаке, необходимо надежно шифровать или защищать. Не нужно забывать, что обеспечение безопасности всегда влияет на производительность системы (в сторону уменьшения) и эффективность ее использования.

8. Схемы резервного копирования и восстановления должны регулярно выполняться для предотвращения потери данных. При этом они тоже должны быть надежно защищены.

9. Надлежащую проверку подлинности, авторизацию и доступ к инструментам обеспечения безопасности необходимо регулярно контролировать.

10. Протоколы шифрования и управления ключами шифрования при передаче данных (в том числе резервных копий) должны постоянно обновляться.

Облачные технологии дают образовательным организациям большие преимущества как в организации учебного процесса, так и в управлении образовательной организацией. Однако образовательные организации по-прежнему и не без оснований обеспокоены вопросами безопасности. Риски при использовании облачных технологий могут представлять собой серьезное препятствие, способное помешать внедрению облачных технологий. Но при грамотном подходе к организации работы в облаке информация будет защищена гораздо лучше, чем локальная информация в образовательной организации.

Литература

1. *Агапов А.Б.* Проблемы правовой регламентации информационных отношений в Российской Федерации // Государство и право. 1993. № 4. С. 125–130.

2. *Аносов В.Д., Стрельцов А.А.* О доктрине информационной безопасности РФ (проект) // Информационной общество. 1997. № 2–3. С. 3–9.

3. *Архипов А.В.* Информационная защита объекта — задача многогранная // Конфидент. 1990. № 1–2. С. 30–31.

4. *Бачило И.Л.* Правовое регулирование процессов информатизации // Государство и право. 1994. № 12. С. 72–80.

5. *Волков С., Булычев В.* Защита деловой репутации от порочащих сведений // Российская юстиция. 2003. № 8. С. 51.

6. *Гиляров Е.М., Янина Е.В.* Информация как объект правового регулирования // Безопасность информационных технологий. 2001. № 3. С. 5–10.

7. *Ефанова Т.И., Иванов А.Б., Савицкий С.К., Хабибулин Э.М.* и др. Информационно-образовательная среда вуза // Новое слово в науке: перспективы развития: мат-лы VII Международной научно-практической конференции. Т. 1. № 1 (7). Чебоксары: ЦНС «Интерактив плюс», 2016. С. 195–199.

8. *Заславский А.А.* Использование моделей «облачных технологий» для дифференциации обучения информатике. // Педагогическое образование и наука. 2012. № 5. С. 53–55.

9. *Заславский А.А.* Возможности облачных технологий, сервисов и приложений в организации эффективной работы с информацией в условиях построения индивидуальной траектории обучения информатике // Инновации и качество лицейского образования: идеи, опыт, практика. 2012. № 1–2 (14). С. 17–20.

10. *Заславский А.А.* Аренда виртуальных серверных ресурсов для реализации научных проектов учащихся // Инфо-Стратегия 2015: Общество. Государство. Образование: сб. мат-лов VII Международной научно-практической конференции. Самара: Книга, 2015. С. 111.

11. *Заславская О.Ю., Заславский А.А.* Дидактический потенциал облачных технологий // Справочник заместителя директора школы. 2014. № 10. С. 47–53.

12. *Khalil H. A. Al-Shqeerat, Mohammad Ali A. Hammoudeh, Mohammad Ijaz Abbasi*. Design and Analysis of an Effective Secure Cloud System at Qassim University // International Journal of Computer Science and Information Security (IJCSIS). 2016. Vol. 14 (8). Pp. 85–90.

13. *Velumadhava Raoa R., Selvamanib K.* Data Security Challenges and Its Solutions in Cloud Computing, in Proc // International Conference on Intelligent Computing, Communication & Convergence (ICCC), Bhubaneswar, Odisha, India, 2015. Pp. 204–209.

Literatura

1. *Agapov A.B.* Problemy' pravovoj reglamentacii informacionny'x otnoshenij v Rossijskoj Federacii // Gosudarstvo i pravo. 1993. № 4. S. 125–130.

2. *Anosov V.D., Strel'czov A.A.* O doktrine informacionnoj bezopasnosti RF (proekt) // Informacionnoj obshhestvo. 1997. № 2–3. S. 3–9.

3. *Arxipov A.V.* Informacionnaya zashhita ob''ekta — zadacha mnogogrannaya // Konfident. 1990. № 1–2. S. 30–31.

4. *Bachilo I.L.* Pravovoe regulirovanie processov informatizacii // Gosudarstvo i pravo. 1994. № 12. S. 72–80.

5. *Volkov S., Buly'chev V.* Zashhita delovoj reputacii ot porochashhix svedenij // Rossijskaya yusticiya. 2003. № 8. S. 51.

6. *Gilyarov E.M., Yanina E.V.* Informaciya kak ob''ekt pravovogo regulirovaniya // Bezopasnost' informacionny'x texnologij. 2001. № 3. S. 5–10.

7. *Efanova T.I., Ivanov A.B., Saviczkij S.K., Xabibulin E'.M.* i dr. Informacionno-obrazovatel'naya sreda vuza // Novoe slovo v nauke: perspektivy' razvitiya: mat-ly' VII Mezhdunarodnoj nauchno-prakticheskoj konferencii. T. 1. № 1 (7). Cheboksary': CNS «Interaktiv plyus», 2016. S. 195–199.

8. *Zaslavskij A.A.* Ispol'zovanie modelej «oblachny'x texnologij» dlya differenciacii obucheniya informatike // Pedagogicheskoe obrazovanie i nauka. 2012. № 5. S. 53–55.

9. *Zaslavskij A.A.* Vozmozhnosti oblachny'x texnologij, servisov i prilozhenij v organizacii e'ffektivnoj raboty' s informaciej v usloviyax postroeniya individual'noj traektorii obucheniya informatike // Innovacii i kachestvo licejskogo obrazovaniya: idei, opy't, praktika. 2012. № 1–2 (14). S. 17–20.

10. *Zaslavskij A.A.* Arenda virtual'ny'x serverny'x resursov dlya realizacii nauchny'x proektov uchashhixsya // Info-Strategiya 2015: Obshhestvo. Gosudarstvo. Obrazovanie: sb. mat-lov VII Mezhdunarodnoj nauchno-prakticheskoj konferencii. Samara: Kniga, 2015. S. 111.

11. *Zaslavskaya O.Yu., Zaslavskij A.A.* Didakticheskij potencial oblachny'x texnologij // Spravochnik zamestitelya direktora shkoly'. 2014. № 10. S. 47–53.

12. *Khalil H. A. Al-Shqeerat, Mohammad Ali A. Hammoudeh, Mohammad Ijaz Abbasi*. Design and Analysis of an Effective Secure Cloud System at Qassim University // International Journal of Computer Science and Information Security (IJCSIS). 2016. Vol. 14 (8). Pp. 85–90.

13. *Velumadhava Raoa R., Selvamanib K.* Data Security Challenges and Its Solutions in Cloud Computing, in Proc // International Conference on Intelligent Computing, Communication & Convergence (ICCC), Bhubaneswar, Odisha, India, 2015. Pp. 204–209.

O.Yu. Zaslavskaya,
A.V. Ivanov

Security Issues When Using Cloud Technologies in Educational Organizations

The article discusses the use of cloud technologies in the activity of an educational organization. The authors analyze possible security risks when using cloud technologies in educational organizations.

Keywords: cloud technologies; management of education; security; information technologies in education; information and educational environment.