Проблемы защиты информации субъектов электронного университета в облачной среде

Фирудин Агаев[1], Гюляра Мамедова[2], Эсмира Алескерова[3]
[1,2,3]Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]*depart10@iit.science.az*, [2]*gyula.ikt@gmail.com*

***Аннотация*— В этой статье определены различные проблемы безопасности электронного образования при предоставлении облачных сервисов и предложены решения по обеспечению мер безопасности. Также обсуждаются различные типы атак на платформы электронного обучения. Исследуются различные модели использования облачных технологий в электронном образовании, угрозы и требования безопасности при использовании этих моделей.**

Ключевые слова— электронный университет, модели доставки облачных услуг, контроль идентификации и аутентификации, защита облачного сервера, MITM атаки, DDoS атака, инсайдерские атаки.

I. ВВЕДЕНИЕ

Электронное обучение на основе облачных технологий – одна из быстро развивающихся информационных технологий, которая предлагает мощные продукты электронного обучения с помощью облачных технологий [1-2]. Облачные технологии имеют многочисленные преимущества по сравнению с существующими традиционными системами электронного обучения, но в то же время безопасность является серьезной проблемой в облачном электронном обучении. Чтобы предотвратить потерю ценных данных пользователей из-за уязвимостей безопасности, необходимо соблюдать соответствующие меры безопасности. Облачные продукты электронного обучения должны удовлетворять потребностям клиентов в безопасности и преодолевать различные угрозы безопасности. В работе мы рассматриваем ключевые проблемы безопасности при использовании облачных вычислений в системах электронного обучения.

II. ОБЛАЧНАЯ АРХИТЕКТУРА ЭЛЕКТРОННОГО ОБУЧЕНИЯ

Облачная архитектура электронного обучения в основном разделена на пять уровней [3], называемых: уровнем аппаратных ресурсов, уровнем программных ресурсов, уровнем управления ресурсами, уровнем сервера и уровнем приложений. Облачная архитектура электронного обучения поясняется на рис. 1.

Уровень аппаратных ресурсов – это самый нижний уровень облачной инфраструктуры, которая обеспечивает вычислительную мощность электронного образования. Чтобы обеспечить бесперебойную работу облачных сервисов для систем электронного обучения, физическая память динамически расширяется, и в любое время масштабируется для добавления дополнительной памяти.

Уровень программных ресурсов включает операционную систему и прикладное программное обеспечение для разработчиков и пользователей облачной инфраструктуры.

Уровень управления ресурсами играет важную роль в слабой взаимосвязи программных и аппаратных ресурсов. С помощью идеи виртуализации она обеспечивает бесперебойное распространение программного обеспечения по требованию для различных аппаратных ресурсов облачной инфраструктуры.

Уровень обслуживания делится на три уровня: IAAS (Инфраструктура как сервис), PAAS (Платформа как сервис) и SAAS (Программное обеспечение как сервис). Эти сервисные уровни помогают облачным клиентам использовать различные виды облачных сервисов, таких как, программный сервис, аппаратный сервис и сервис инфраструктуры.

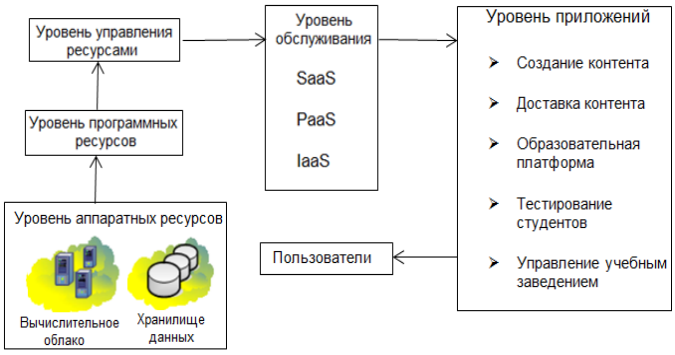

Рис.1. Облачная архитектура электронного образования.

Уровень приложений отличается от всех других уровней в архитектуре электронного обучения на основе облачных вычислений, поскольку создает основу компонентов для электронного обучения и служит для создания учебного контента, доставки контента,

DOI: 10.25045/NCInfoSec.2019.28

образовательной платформы, оценки обучения и управления образованием.

III. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ СЕРВИСОВ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ ДЛЯ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ

Как было показано выше, существуют три модели доставки облачных услуг: 1. Программное обеспечение как сервис (SaaS), 2. Платформа как сервис (PaaS) (), 3. Инфраструктура как сервис (IaaS). В этой статье рассматриваются вопросы безопасности в каждой из этих групп.

Программное обеспечение как сервис (SaaS) – позволяет совместно работать нескольким пользователям с готовым программным обеспечением. Поэтому в SaaS пользователь полностью зависит от поставщика программного обеспечения. Для обеспечения надлежащих мер безопасности поставщик программного обеспечения должен обеспечить безопасность учебных данных, так, чтобы было невозможно нескольким пользователям видеть данные друг друга. Учебное заведение должно быть уверенным, что поставщик облачных сервисов будет обрабатывать данные только в соответствии с его инструкциями, что он принял соответствующие меры, чтобы исключить неавторизованный доступ к данным, их изменение или уничтожение.

Платформа как сервис (PaaS) предоставляют вычислительную платформу и системное программное обеспечение как услугу. PaaS предоставляет сервисные услуги для разработчиков программного обеспечения. Сюда можно отнести такие платформы, как, Google App Engine, Salesforce, Windows Azure и др., позволяющие создавать программы и корпоративные сайты на языках Java и Python. Поставщики PaaS предоставляют услуги для разработки приложений, развертывания, коллективного сотрудничества, интеграции веб-сервисов и тестирования [4].

Основными угрозами безопасности уровня PaaS являются местоположение данных и привилегированный доступ. В США и во многих странах ЕС были установлены универсальные стандарты безопасности и законы о конфиденциальности данных для проблем с размещением данных. Например, общим регламентом по защите данных (GDPR — General Data Protection Regulation) от 27 апреля 2016 г., действующем во всех странах ЕС, они никогда не позволяют конфиденциальным данным перемещаться из страны [5-6]. За нарушение правил обработки персональных данных, штрафы достигают миллионы евро.

Основываясь на местоположении данных, модель PaaS обеспечивает надежность для своих клиентов. Для обеспечения надежного хранения данных на уровне PaaS, пользователь должен выбрать надежный метод шифрования для доступа к данным, поддерживать высокую стандартную конфиденциальность данных, требовать от облачного провайдера юридически оформленные договорные обязательства механизмов обеспечения безопасности. Поставщик облачных услуг должен иметь технические решения для предотвращения несанкционированного доступа пользователей и поддерживать принцип разделения обязанностей для привилегированных пользователей с целью предотвращения и обнаружения вредоносной инсайдерской деятельности.

При хранении зашифрованных данных в облачном хранилище ключи дешифрования должны надежно храниться в других дезинтегрированных системах [7-8]. Если облачная пользовательская система позволяет поставщику облачных услуг обрабатывать незашифрованные данные, поставщик облачных услуг должен гарантировать, что данные будут защищены от несанкционированного доступа как внутри, так и снаружи.

Инфраструктура как сервис (IaaS) позволяет использовать множество ресурсов, таких как серверы, хранилища, сети и другие вычислительные ресурсы, представляет собой хостинг для виртуальной машины. В случае, если IaaS обеспечивает полный контроль и управление ресурсами, пользователи могут с безопасностью запускать любое программное обеспечение на выделенных ресурсах. В этом случае, между пользователем и облачным провайдером заключается соглашение об уровне сервиса SLA (Service Level Agreement), в котором содержится описание предоставляемых услуг, прав и обязанностей сторон. В этом соглашении содержится детальное описание предоставляемых сервисов, методов и средств контроля по обеспечению безопасности информации.

Основными видами угроз в электронном образовании при предоставлении IaaS услуги являются DDoS атаки (Distributed Deny of Service Attack), MITM атака (Man In The Middle), DNS атаки, и др. Цель DDoS атаки заключается в том, чтобы сделать облачную услугу недоступной для авторизованного пользователя. В этом случае злоумышленниками используется SYN-флуд (запросы на подключение по протоколу TCP), при котором весь канал сервера просто забивается запросами на подключение. SYN-флуд является одним из разновидностей сетевых атак типа «отказ в обслуживании», который заключается в отправке большого количества SYN-запросов, переполняя на облачном сервере очередь на подключение.

Другой распространенной угрозой при предоставлении IaaS услуги является MITM атака, когда злоумышленник внедряет себя между двумя законными пользователями сети. Злоумышленник устанавливает соединение между двумя пользователями и пытается завладеть информацией, пересылаемой ими друг другу [9].

В последнее время в облачной среде, использующей IaaS сервис, хакерами применяется такой вид атаки, известный как DNS атака, при котором хакер перенаправляет пользователя на другую виртуальную

машину облака вместо исходного адреса, который он ожидает. Ничего не подозревающий пользователь соединяется с хостом нарушителя и, полагая, что работает на сайте учебного заведения, вводит конфиденциальную информацию на подложный IP адрес. При DNS атаке злоумышленник получает возможность мгновенно менять параметры транзакции, а также страницы запроса пользователя совершенно прозрачно для жертвы.

IV. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ СЕРВИСОВ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ ДЛЯ ЭЛЕКТРОННОГО ОБРАЗОВАНИЯ

При предоставлении облачных сервисов для электронного университета, для обеспечения безопасности информации, особое внимание требует уделить защите аппаратных и виртуальных устройств обработки данных, а также каналов связи. Необходимо обеспечить следующие критерии безопасности [10-11]:

- контроль идентификации и аутентификации субъектов и объектов доступа;
- защиты машинных носителей информации;
- обеспечение необходимого уровня криптографической и антивирусной защиты хранимой и передаваемой информации;
- защита облачного сервера, средств связи и передачи данных;
- принятие мер по межсетевому экранированию.

Чтобы защитить данные от утечки конфиденциальной информации, необходимо применять жесткие методы шифрования сетевого трафика для управления потоком данных в сети: Secure Socket Layer (SSL) и Transport Layer Security (TLS). Эти уровни обеспечения безопасности позволят защитить от традиционных сетевых проблем, таких как атаки MITM, IP-спуфинг, сканирование портов, обнюхание пакетов и т. д.

Атаки сегодня стали сложными и многоуровневым, злоумышленники выбирают конкретные цели и долго готовятся к нападению, чтобы ударить именно в наиболее уязвимые элементы. Эволюция интернет-угроз закономерно повлияла и на развитие средства противодействия им. Сегодня наиболее эффективными инструментами защиты облачных ресурсов от внешних атак из сети – это решения класса Cloud Access Security Broker (CASB), направленные на удовлетворение новых требований безопасности. CASB представляет собой унифицированный инструмент контроля за всеми облачными приложениями, ресурсами и сервисами, контролирует взаимодействие между облачными приложениями (доступ, трафик, загрузку и хранение данных), сервером и внешними пользователями, позволяет выявлять потенциальные угрозы и ориентирован на высокий уровень защиты облачной среды [12-13]. CASB предотвращает несанкционированные действия пользователей, обнаруживает аномальную активность, в том числе, связанную с действиями различных вредоносных программ. По данным, опубликованным агентством Gartner в 2019 г., лидерами рынка обеспечения безопасности облачных услуг являются: Skyhigh Networks, Netskope, Symantec [14-15].

А появившийся недавно пакет программ CloudSOC Security for Cloud Apps [16] контролирует в реальном времени транзакции с санкционированными (разрешенными) и несанкционированными облачными приложениями; осуществляет визуализацию карты активности пользователей для быстрого анализа их действий; защищает от угроз, основанных на обширной аналитике поведения пользователей. Он обеспечивает богатую наглядность, контроль перемещения данных и сложную аналитику для выявления и борьбы с киберугрозами во всех ваших облачных сервисах.

Применение инструментов CASB в электронном образовании позволят, анализируя журналы «регистрации» и «геолокации», данные о времени совершения тех или иных действий в «облаке», отслеживать действия пользователей выявлять угрозы в реальном времени, идентифицировать небезопасные приложения. В эти пакеты встроены средства машинного обучения, предусматривающие возможность отслеживать поведенческие действия пользователей и их отклонение от нормы. Посредством анализа индикаторов риска, таких как: небезопасные IP-адреса, сбои при регистрации, уровень активности, неактивные учетные записи, сценарии «невозможных путешествий» и их локация, своевременно выявлять злоумышленников в сети.

ЗАКЛЮЧЕНИЕ

Проблема доступности данных в электронном образовании является основным препятствием для обеспечения безопасности облачных данных. Литературное исследование ясно показывает риски в электронном обучении на основе облачных вычислений, а также его модели предоставления услуг и эффективные решения для каждой атаки. Перечисленные проблемы безопасности важны для управления и новой методологии разработки безопасного электронного обучения на основе облачных вычислений в будущем.

Основной целью работы является выяснение ключевых проблем безопасности, возникающих при реализации облачных вычислений для систем электронного обучения. Разработка систем электронного обучения должна осуществляться с использованием методов безопасности и международно признанных стандартов. Система должна реализовать службы безопасности, такие как, аутентификация, шифрование, контроль доступа, управление пользователями и их разрешениями.

ЛИТЕРАТУРА

[1] N. Antonopoulos, L. Gillam. Cloud Computing: Principles, Systems and Applications. London: Springer-Verlag, 2010. 379 p

[2] Н. Склейтер. Облачные вычисления в образовании. Аналитическая записка. Пер. с англ. Институт ЮНЕСКО по информационным технологиям в образовании (ИИТО ЮНЕСКО). 2010. http://iite.unesco.org/pics/publications/ru/files/3214674.pdf.

[3] К. Фогарти “Облачные вычисления: определения и решения,” Открытые системы, 2011, № 3. http://www.osp.ru/cio/2011/03/13007508.

[4] В. Ф. Шаньгин, Информационная безопасность компьютерных систем и сетей. – М.: ИД «ФОРУС»: Инфра-М, 2008. – 416 с.

[5] https://ec.europa.eu/info/law/law-topic/data-protection_en

[6] А. Пазюк, М. Соколова. Защита персональных данных: международные принципы и стандарты. 2015. 23 p. https://www.researchgate.net/publication/281459857

[7] А.В. Ерыгин Анализ эффективности систем предотвращения утечек конфиденциальной информации из локальных сетей. Вестник СибАДИ, выпуск 2 (20), 2011, с. 40-47.

[8] M.Jensen, J.Schwenk, N.Gruschka, & L.Iacono “On technical security issues in cloud computing,” IEEE International Conference on Cloud Computing,pp.109-116, 2009.

[9] F. Callegati, W. Cerroni, & M. Ramilli “Man-in-the-Middle Attack to the HTTPS Protocol,” IEEE Security & Privacy, 7(1), pp. 78-81, 2009.

[10] E. B. Fernandez, N. Yoshioka, and H. Washizaki, “Patterns for cloud firewalls”, Procs. of AsianPLoP (AsianPattern Languages of Programs), 2014

[11] Исаев Е.А., Думский Д.В., Самодуров В.А., Корнилов В.В. Обеспечение информационной безопасности облачных вычислений Математическая биология и биоинформатика , 2015. Т. 10. № 2. С. 567–579.

[12] H. Reza, M. Sonawane, "Enhancing mobile cloud computing security using steganography," Journal of Information Security, 2016, pp. 245-259.

[13] https://www.anti-malware.ru/analytics/Market_Analysis/cloud-access-se-curity-broker

[14] https://www.gartner.com/reviews/market/cloud-access-security-brokers/co-mpare/symantec-blue-coat-vs-skyhigh-networks

[15] C. Lawson, S.Riley “Magic Quadrant for Cloud Access Security Brokers”. Gartner. 29 October 2018. https://www.bsigroup.com/globalassets/local-files /enie/csir/resources/whitepaper/1810-magic_quadrant_for_casb.pdf

[16] https://www.symantec.com/content/dam/symantec/docs/data-sheets/cloud-soc -gateway-en.pdf

INFORMATION SECURITY PROBLEMS OF E-UNIVERSITY IN CLOUD ENVIRONMENT

Firudin Aghayev[1], Gyulara Mammadova[2], Esmira Aleskerova[3]

[1,2,3]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]depart10@iit.science.az, [2]gyula.ikt@gmail.com

Abstract– This article identifies various security issues of e-education in the provision of cloud services and proposes solutions to ensure security measures. Various types of attacks on e-learning platforms are also discussed. Various models of the use of cloud technologies in electronic education, threats and security requirements when using these models are investigated.

Keywords– *electronic university, cloud service delivery models, identification and authentication control, cloud server protection, MITM attacks, DDoS attacks, insider attacks.*