Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК004.56

Дугушкина
Ольга Александровна

Обеспечение безопасности персональных данных в системах дистанционного обслуживания пользователей

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

_____

Научный руководитель:
Борискевич Анатолий Антонович
доктор технических наук,
профессор, доцент

_____

Минск 2016

ВВЕДЕНИЕ

На сегодняшний день одним из наиболее перспективных способов оптимизации ИТ-инфраструктуры являются облачные вычисления (англ. cloud computing).

Облачные вычисления и облачные системы хранения данных завоевали популярность как наиболее удобный способ передачи информации и предоставления функциональных средств в Интернете. Они предлагают широкие возможности вычисления, обработки и хранения данных. Благодаря облачным вычислениям, компании могут предоставлять пользователям удаленный динамический доступ к услугам, вычислительным ресурсам и приложениям через сеть Интернет. Вычислительные облака состоят из тысячи серверов, размещенных в физических и виртуальных центрах обработки данных, обеспечивающих работу десятков тысяч приложений, которые одновременно используют миллионы пользователей. По сравнению с традиционным подходом, облачные вычисления позволяют управлять более крупными инфраструктурами, обслуживать различные группы пользователей в пределах одного облака.

Облачная инфраструктура дает пользователям возможность менять, находящиеся в их распоряжении, ресурсы и вычислительные мощности, таким образом, чтобы они соответствовали их потребностям, в соответствии с рабочей нагрузкой. Регулирование вычислительных мощностей осуществляется как вручную, так и с помощью специализированных программ, автоматически регулирующих вычислительные мощности в соответствии с текущими потребностями.

При наличии очевидных достоинств, основным сдерживающим фактором при реализации концепции облачных вычислений является вопрос информационной безопасности, так как данные хранятся и обрабатываются на удаленных, не контролируемых пользователями информационных ресурсах. Решение по обеспечению информационной безопасности полностью ложится на провайдер, который обязан позаботиться об охране доступа, в том числе и о физической безопасности, а также об устойчивости к сбоям.

В настоящей работе предложен двухэтапный метод аутентификации пользователя при доступе к облачным ресурсам. Рассмотрена аутентификация как услуга в облачных вычислениях, которую можно использовать для повышения анонимности пользователя, надежности и практичности использования облачных сервисов.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи исследования

Цель диссертационной работы заключается в методике анализа угроз в облачных вычислениях и методах их предотвращения, разработке алгоритма аутентификации пользователя при доступе к услугам облачных вычислений.

Для достижения поставленной цели необходимо было выполнить следующие задачи:

1. Провести анализ облачных моделей доступа, классификацию облачных сервисов.
2. Провести анализ угроз, характерных облачной среде и методов их предотвращения.
3. Разработать алгоритм аутентификации пользователя при доступе к услугам облачных вычислений.

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует подразделу 5.2. «системные решения, архитектура, методологическое и аппаратно-программное обеспечение высокопроизводительных параллельных и распределенных информационно-коммуникационных процессов, сетей и систем, их информационная безопасность» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2011 – 2015 гг., утверждённых Постановлением Совета Министров Республики Беларусь 19 апреля 2010г., № 585. Работа выполнялась в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники».

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликовано 2 работы, в том числе 2 статьи в сборниках материалов конференций.

Положения, выносимые на защиту

1. Методика анализа угроз безопасности в облачных вычислениях и методах их предотвращения.
2. Разработка алгоритма аутентификации пользователей при доступе к облачным ресурсам с целью повышения уровня безопасности персональных данных пользователя.

Личный вклад соискателя ученой степени

Содержание диссертации отражает личный вклад автора. Заключается в анализе существующих угроз безопасности в облачных вычислениях и методах их предотвращения.

Определения целей и задач исследований, интерпретация и обобщение научных результатов проводились совместно с научным руководителем диссертации профессором, доктором технических наук, доцентом Борискевичем Анатолием Антоновичем.

Апробация диссертации и информация об использовании ее результатов

Основные положения и результаты исследований докладывались и обсуждались на научных и научно-практических конференциях разного уровня: Международной военно-научной конференции (Минск, 23.04.2015-24.04.2015), XX Международной научно-практической конференции «Комплексная защита информации» (Минск, 19.05.2015-21.05.2015).

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении и общей характеристике работы обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования, цель и задачи, формулируются основные положения диссертации, выносимые на защиту.

Первая глава «Анализ архитектуры облачных вычислений» носит теоретический характер, состоит из 4 разделов. В ней определяется следующее:

– в соответствии с руководством национального института стандартов и технологий США дается определение облачных вычислений, описываются основные характеристики облачных вычислений, досоинства и недостатки;

– приводится эталонная модель архитектуры облачных вычислений (NIST Definition of Cloud Computing), которая представляет собой три сервисных модели (SaaS, PaaS, IaaS), четыре модели развертывания (частное, общее, публичное, гибридное облако) и пять основных характеристик, связывает различные облачные сервисы и отображает их на общую модель, действует как дорожная карта (роадмэп) индустрии ИТ для понимания, выбора, проектирования и/или развертывания облачной инфраструктуры;

– приводятся основные параметры безопасности, которые включают в себя: аутентификацию и авторизацию, доступность, конфиденциальность, управление идентификацией , мониторинг безопасности и обработка инцидентов, управление политиками безопасности, приватность; рассмотрен ряд вопросов, которые необходимо учитывать для обеспечения безопасности при работе с облачными вычислениями.

Вторая глава носит практико-ориентированный характер, состоит из 6 разделов. В ней определяется следующее:

– Рассмотрим ряд факторов, которые должны всегда учитываться в качестве основы построения облачной конфигурации: затраты и ресурсы, надёжность, производительность, целостность, конфиденциальность, доступность, правовые и нормативные ограничения;

– все аспекты безопасности должны быть отражены в документе «Политика информационной безопасности организации»

• ряд руководящих принципов для обеспечения безопасности при разработке программного обеспечения, в процессах управления ИТ инфраструктурой, и других операционных процедурах;

• политика допустимого использования ресурсов для каждой категории пользователя: от внутренних операций, выполняемых администратором до действий конечных пользователей. Этот раздел должен идентифицировать категории использования ресурсов, определить

критичную информацию, доступ к которой запрещен, обозначить последствия для нарушений;

• ряд стандартов безопасности для всех аспектов облачной архитектуры, от миграции данных до операционной деятельности.

– стандарты безопасности для облачных вычислений должны включать в себя: средства управления доступом, управление реагированием на инциденты безопасности, резервное копирование системной и сетевой конфигурации, тестирование безопасности, шифрование данных и связи, политика строгих паролей, непрерывный мониторинг;

– угрозы облачных вычислений: трудности при перемещении обычных серверов в вычислительное облако, динамичность виртуальных машин, уязвимости внутри виртуальной среды, защита бездействующих виртуальных машин, защита периметра и разграничение сети, угрозы облачных вычислений;

– рассмотрено правовое обеспечение облачных вычислений. Во многих странах мира разрабатываются стандарты и руководства, содержащие рекомендации по использованию облачных вычислений. Основное внимание уделяется вопросам обеспечения информационной безопасности и защите персональных данных.

Третья глава носит практический характер, состоит из 4 разделов. В ней определяется следующее:

– разработан и описан алгоритм двухэтапной аутентификации пользователя облачных вычислений, который обеспечивает более надежную защиту персональных данных пользователя от несанкционированного доступа и кражи злоумышленником посредством использования дополнительных параметров идентификации пользователя;

– Анализ безопасности: в двухэтапном методе аутентификации используется динамический ключ, который отправляется на email пользователя, что существенно повышает безопасность по сравнению с базовой (однофакторной) аутентификацией. Данный ключ генерируется из хеш-таблицы. Также значительно повысить безопасность позволяет ограничение времени и количества попыток конкретного сеанса. Т.е. после некоторого времени и количества попыток ввода доступ к ресурсам становится невозможен и необходимо заново входить в систему;

– Представлена модель архитектуры аутентификации как услуги (Authentication-as-a-Service (AaaS)), в которой пользователи авторизуются в AaaS для получения ключа (token). Используя этот ключ пользователь может перемещаться в различных сервисах (everything as-a-service – XaaS) поставщика без перерегистрации и повторной аутентификации. Это позволяет повысить анонимность пользователя в используемых им сервисах, повысить простоту и практичность работы в облачной инфраструктуре

ЗАКЛЮЧЕНИЕ

В диссертации описана эталонная модель архитектуры облачных вычислений (NIST Definition of Cloud Computing), которая представляет собой три сервисных модели (программное обеспечение как услуга (SaaS), платформа как услуга (PaaS), инфраструктура как услуга (IaaS)), четыре модели развертывания (частное облако, общее облако, публичное облако, гибридное облако) и пять основных характеристик (самообслуживание по требованию, широкий (универсальный) сетевой доступ, объединение ресурсов, мгновенная эластичность ресурсов, измеряемый сервис), связывает различные облачные сервисы и отображает их на общую модель, действует путеводителем индустрии ИТ для понимания, выбора, проектирования и/или развертывания облачной инфраструктуры.

Рассмотрен ряд факторов, которые должны учитываться в качестве основы построения облачной инфраструктуры, для обеспечения соответствующей безопасности с учетом существующих угроз и атак в облачной среде.

Рассмотрено правовое обеспечение облачных вычислений. Во многих странах мира разрабатываются стандарты и руководства, содержащие рекомендации по использованию облачных вычислений. Основное внимание уделяется вопросам обеспечения информационной безопасности и защите персональных данных.

Разработан и описан алгоритм двухэтапной аутентификации пользователя облачных вычислений, основанный на генерации и проверке динамического секретного ключа с помощью вычисления хэш-функции, который обеспечивает более надежную защиту персональных данных пользователя от несанкционированного доступа и кражи злоумышленником посредством использования дополнительных параметров идентификации пользователя.

Представлена модель архитектуры аутентификации как услуги (AaaS), в которой пользователи авторизуются в AaaS для получения ключа (token). Используя этот ключ пользователь может перемещаться в различных сервисах (XaaS) поставщика без перерегистрации и повторной аутентификации. Это позволяет повысить анонимность пользователя в используемых им сервисах, повысить простоту и практичность работы в облачной инфраструктуре.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1-А. Дугушкина, О.А. Системный подход к технической защите информации / О.А. Дугушкина. // Международная военно-научная конференция: тезисы докладов УО ВАРБ. Минск, 23-24 апреля 2015 г. – Минск, 2015 – с.378 .

2-А. Дугушкина, О.А Особенности формирования локальных нормативных правовых актов по защите информации и внедрению систем информационной безопасности / О.А. Дугушкина. // Комплексная защита информации: материалы XX научно-практической конференции. Минск,19-21 мая 2015 г. – Минск: РИВШ, 2015 – с 75.