E CONF SERIES

International Conference on Modern Science and Scientific Studies
Hosted online from Madrid, Spain
Website: econfseries.com 20th July 2025

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНОЙ СРЕДЕ

Ботиров С. Р.
магистрант ТУИТ имени Мухаммада ал-Хоразмий

Зоирова М. А.
студент бакалавра

В докладе рассматриваются угрозы информационной безопасности в облачной среде. Описаны задачи необходимые для выработки подходов к обеспечению информационной безопасности в облачной среде.

The report reviews the threats of information security in the cloud environment. The necessary tasks for developing approaches to ensuring information security in a cloud environment are described.

Облачные вычисления имеют четыре модели предоставления услуг и три основных моделей развертывания. Каждая модель предоставления услуг имеет различные возможные реализации, что усложняет разработку стандартной модели безопасности для каждой модели предоставления услуг. Более того, эти модели предоставления услуг могут сосуществовать в одной облачной платформе, что приводит к дальнейшему усложнению процесса управления безопасностью.

Архитектура облачных вычислений основана на web-технологиях, и для нее также актуальны угрозы, связанные с уязвимостями сетевых протоколов, серверов приложений и операционных систем: Использование не безопасных программных интерфейсов (API); утечка данных; утрата данных; угрозы, связанные с применением виртуальной сред; несанкционированный доступ (НСД) к учетным записям или сервисам клиентов, основная опасность НСД сегодня исходит прежде всего от самого облака, поскольку методы и техники защиты на уровне виртуальной среды еще недостаточно развиты.

Облачные вычисления основаны на сетевой централизованности, виртуализации и связанных с этими факторами – динамичностью и гибкостью при создании новых функций приложений. Однако уже на нынешнем этапе развития облачных вычислений выявлен ряд уязвимостей, связанных, не только с классическими угрозами для распределенных автоматизированных систем, но и с принципиально новыми угрозами, порожденными спецификой виртуализации.

Механизмы виртуализации основаны на разделении общих ресурсов. При этом появляется огромное количество каналов межпрограммного взаимодействия, которые связаны с защищаемыми информационными ресурсами и не поддаются анализу. Быстрое и гибкое изменение архитектуры предоставляет нарушителю больше возможностей, чем в классической архитектуре.

Информационные системы, использующие механизмы виртуализации, снабжаются большим набором механизмов безопасности и правил их использования. Однако выявлены многочисленные уязвимости, связанные с невозможностью и (или) неумением анализировать непротиворечивость и другие свойства совместного применения многочисленных механизмов безопасности. То есть синергетический эффект от их совместного использования может быть и отрицательным.

Появились распределенные вирусы и возможности скрытого взаимодействия виртуальных систем на одном физическом сервере. Эти «скрытые виртуальные туннели» для злоумышленных целей еще требуют своего выявления, осознания, классификации и необходимости разработки упреждающих и блокирующих действий пользователей облачных услуг.

Среди первоочередных задач по выработке подходов к обеспечению информационной безопасности облаков необходимо отнести следующие:

1. Исследование вопросов наличия уязвимостей виртуальных сред;
2. Построение классификации уязвимостей виртуальных сред;
3. Разработку типовой модели угроз для виртуальных сред;

Одной из актуальных задач, возникающих при создании и эксплуатации такого рода информационных систем, является обеспечение возможности

использования в их составе недоверенного программного обеспечения (ПО) с сохранением соответствия самих информационных систем требованиям по безопасности. В качестве возможного решения может быть рассмотрено использование технологии виртуализации, позволяющей изолировать потенциально опасное ПО.

При внедрении технологий виртуализации стоит выделить два ключевых вопроса в контексте ИБ. Первый – это обеспечение безопасности конфиденциальной информации с учетом угроз, специфичных для среды виртуализации; второй, не менее существенный, связан с выполнением требований регуляторов в части защиты информации. В результате возникает непростая дилемма – как обеспечить безопасность конфиденциальной информации и соблюсти требования законодательства, но при этом не свести на нет все преимущества от использования технологий виртуализации.

Обеспечение безопасности облачных сервисов во многом делегируется самому провайдеру облачных вычислений, однако несмотря на это, он не отвечает за то, как пользуются его сервисами. Слабым местом любых облачных вычислений являются люди, которые их используют, и среда доступа от облака до конечных пользователей. Использование гибридной модели развертывания, комбинируя с много-облачной стратегией в связке с принципом диверсности позволит минимизировать риски нарушения информационной безопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. T. Erl, Cloud Computing: Concepts, Technology & Architecture Published May 2013.
2. J. Rhoton, Cloud Computing Protected: Security Assessment Handbook Published January 2013.