РАСПРЕДЕЛЕНИЕ УРОВНЕЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ СЕРВИСАХ

Р.Д. Авсеенко, Д.С. Кукла

Облачные вычисления изменили способ доставки и использования ИТ-решений конечными пользователями, так как они предоставляют такие услуги как хранилище данных, базы данных, облачные вычисления и многое другое. Большинство современных компаний используют облачные сервисы в своей деятельности ввиду их масштабируемости и удобства эксплуатации. Популяризация облачных технологий и сервисов поставила вопрос об обеспечении безопасности пользовательской информации. Поэтому улучшение безопасности является наиболее приоритетным направлением при построении различных информационных систем и сетей.

В рамках данного исследования было проанализирована возможность построения безопасной архитектуры на основе облачного сервиса Amazon Web Service (AWS). Фундаментальной практикой обеспечения безопасности AWS является

«defense-in-depth», которая реализуется с помощью набора сервисов, основываясь на базовых принципах:

1) контроль доступа – определение, соблюдение и аудит полномочий пользователей (сервис AWS Identity and Access Management и др.);

2) обнаружение угроз – выявление угроз и их устранение до появления последствий (сервис Amazon Guard Duty и др.);

3) защита инфраструктуры – обеспечение сетевой безопасности, фильтрация трафика (сервисы AWS Network Firewall, AWS Shield и др.);

4) защита данных – обеспечение конфиденциальности и целостности информации (сервис AWS Key Management System);

5) реагирование на угрозы безопасности – анализ потенциальных проблем (сервис Amazon Detective и др.).

Необходимо отметить, что облачный сервис Amazon AWS предоставляет множество функций, обеспечивающих управление доступом, контроль трафика, анализ уязвимостей. Так, например, Сервис AWS Identity and Access Management (IAM) предоставляет возможности безопасного управления доступом к сервисам и ресурсам AWS. Используя IAM, можно создавать пользователей и группы, управлять ими, а также использовать разрешения, чтобы предоставлять или запрещать доступ к различным ресурсам. В свою очередь AWS Network Firewall – это управляемая сервис, который упрощает развертывание основных средств защиты сети. Сервис AWS Key Management Service (KMS) обеспечивает централизованный управление криптографическими ключами, используемыми для защиты данных. Этот сервис использует для защиты ключей аппаратные модули безопасности (HSM).

Благодаря множеству предоставляемых сервисов AWS позволяет автоматизировать задачи обеспечения безопасности, решаемые вручную. Данные сервисы тесно интегрированы друг с другом и создают архитектуру построения безопасной, высокопроизводительной, гибкой и эффективной инфраструктуры приложений [1–3].

Литература

1. AWS Security Fundamentals [Электронный ресурс]. – Режим доступа: https://www.aws.training/Details/eLearning?id=34259 – Дата доступа: 02.05.2021.

2. AWS Cloud Security [Электронный ресурс]. – Режим доступа: https://aws.amazon.com/ru/products/security/?nc=sn&loc=2 – Дата доступа: 02.05.2021.

3. Информационная безопасность в AWS [Электронный ресурс]. – Режим доступа: https://www.youtube.com/watch?v=7RRkSTSWOMo&t=1602s – Дата доступа: 02.05.2021.