# АРХИТЕКТУРА ПРОТОТИПА АВТОНОМНОЙ СИСТЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И КАЧЕСТВА ОБСЛУЖИВАНИЯ ПРОГРАММНО-УПРАВЛЯЕМОЙ ИНФРАСТРУКТУРЕ МУЛЬТИОБЛАЧНОЙ ПЛАТФОРМЫ

**Парфёнов Д.И. канд. техн. наук, Дедюрин В.В., Шардаков В.М.**
**Оренбургский государственный университет**

В настоящее время доля использования технологии облачных вычислений для размещения приложений и сервисов в крупных коммерческих и государственных организациях, в том числе на промышленных предприятиях (в областях электроэнергетики, машиностроения, добычи и переработки полезных ископаемых и т.п.) постоянно растет [1-3]. При этом в виртуальную инфраструктуру переносят не только публичные ресурсы организации, но и сервисы, отвечающие за критически важные бизнес процессы, требующие обеспечения заданного качества обслуживания (QoS), а так же необходимого уровня информационной безопасности. Инфраструктура традиционных центров обработки данных (ЦОД) не позволяет в полной мере обеспечить гибкое управление сетевыми и вычислительными ресурсами [4-5]. Это в свою очередь негативно сказывается на параметрах, влияющих на работу облачных приложений и сервисов [6-8].

В рамках настоящего исследования разработан прототип автономной системы обеспечения кибербезопасности и качества обслуживания. Предложенное решение построено на базе современных подходов, используемых при организации виртуальной программно-управляемой инфраструктуры мультиоблачной платформы. В частности для организации базовой инфраструктуры среды передачи данных предлагаемого решения выбрана программно-конфигурируемая сеть (Software-defined networking, SDN). В свою очередь для эффективного использования сетевых ресурсов внутри построенной инфраструктуры использован подход, основанный на виртуализации сетевых функций (Network function virtualization, NFV).

Разработанный прототип является модульным и масштабируемым решением, что позволяет интегрировать его в состав любой системы управления облачными вычислениями. Прототип включает в себя следующий ряд программных компонентов:

1) Модуль глубокого анализа данных, который осуществляет сбор необходимой для принятия решений о фильтрации трафика информации на сетевых и вычислительных узлах мультиоблачной платформы.

2) Модуль контроллера сетевой безопасности, который на основе алгоритма межсетевого экранирования осуществляет управление правилами доступа к ресурсам в сетевой среде мультиоблачной платформы.

3) Модуль обеспечения качества обслуживания в своей работе использует алгоритм самоорганизации управления адаптивной маршрутизацией сетевого трафика в программно-конфигурируемой сети для управления потоками данных приложений и сервисов в мультиоблачной платформе.

4) Модуль управления инфраструктурой мультиоблачной платформы, осуществляет размещение приложений и сервисов в сетевой среде мультиоблачной платформы.

Разработанные модули адаптированы для работы контейнеров на базе Docker, что позволяет быстро разворачивать их в сетевой среде мультиоблачной платформы. Архитектура предлагаемого решения представлена на рисунке 1.

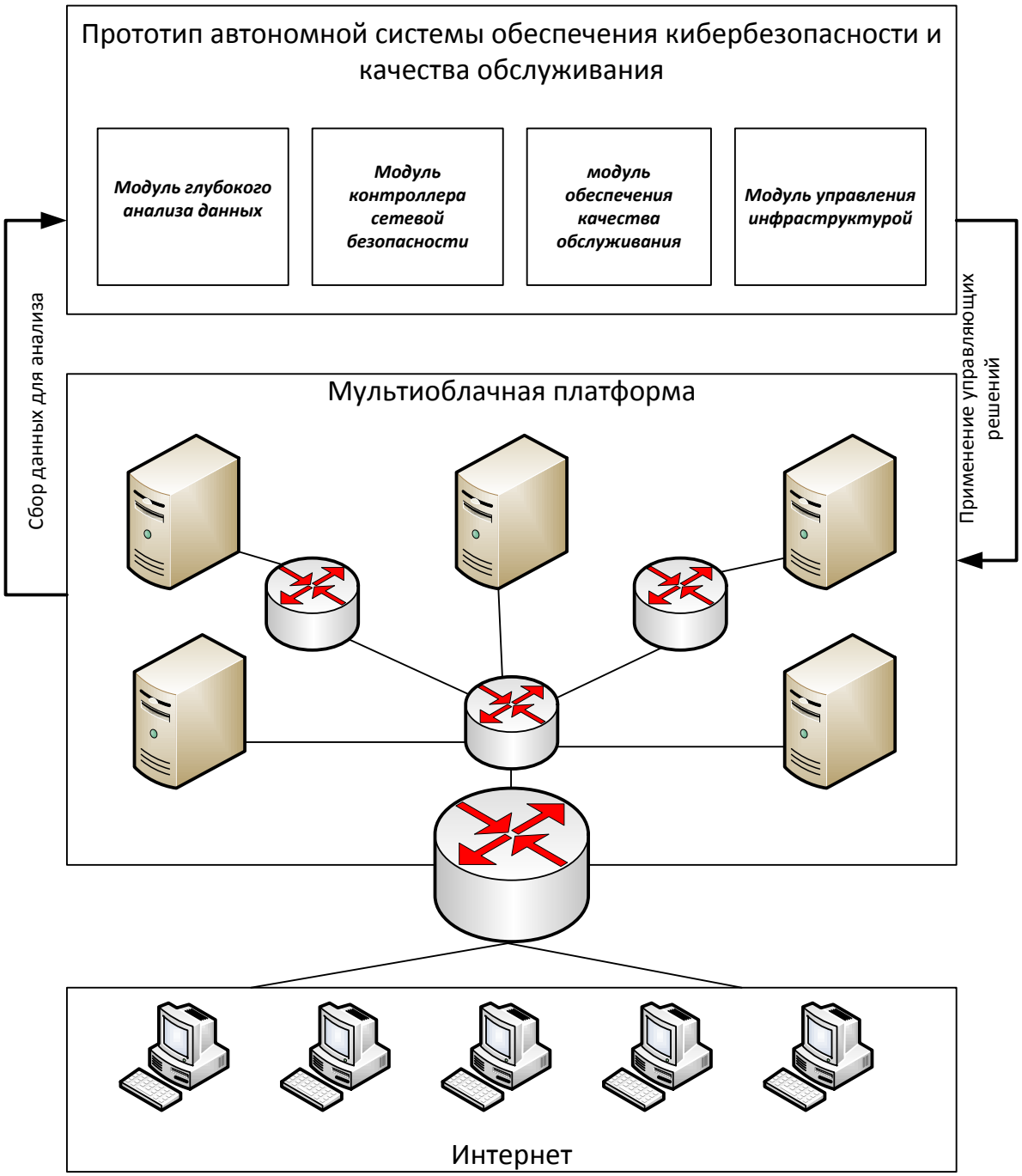


Рисунок 1 – Архитектура прототипа автономной системы обеспечения кибербезопасности и качества обслуживания программно-управляемой инфраструктуре мультиоблачной платформы

Для исследования разработанного прототипа на базе Оренбургского государственного университета построена экспериментальная площадка, включающая в себя два виртуальных ЦОД. В первом виртуальном ЦОД была развернута мультиоблачная платформа (целевая среда кибератаки), построенная на базе OpenStack. Внутри мультиоблачной платформы запущен набор типовых о приложений и сервисов (цели кибератаки) характерных для корпоративных пользователей. Для реализации сценария самой кибератаки на базе второго виртуального ЦОД были определены два сегмента сети. В состав первого сегмента входили легитимные пользователи, отправляющие запросы к целевым приложениям в рабочем режиме. Во втором сегменте была развернуты вычислительные узлы (атакующие агенты), реализованные на базе виртуальных машин и генерирующие вредоносный трафик, направленный к приложениям мультиоблачной платформы.

Для исследования особенностей работы прототипа в экспериментальном исследовании использовались потоки вредоносного трафика различной интенсивности. Кроме того для оценки эффективности предлагаемого решения в плане обеспечения качества обслуживания поступающих от легитимных пользователей проводилась оценка нарушений требований QoS и измерялось время отклика приложений и сервисов внутри облачной системы. Сопоставление результатов полученных при работе прототипа (Активный режим) проводилось с и типовыми модулями обычной облачной системы OpenStack (Пассивный режим). Результаты экспериментального исследования представлены в таблице 1

Таблица 1 - Результаты экспериментального исследования

| № эксперимента | Скорость поступления вредоносного трафика, Гбит/с. | Время отклика приложений и сервисов внутри облачной системы, мс | | Процент нарушений требований QoS, % | |
|---|---|---|---|---|---|
| | | Активный режим | Пассивный режим | Активный режим | Пассивный режим |
| 1 | 0,10 | 45 | 90 | 0,01 | 0,10 |
| 2 | 0,20 | 48 | 120 | 0,20 | 0,20 |
| 3 | 0,30 | 50 | 150 | 0,50 | 30 |
| 4 | 0,40 | 60 | 180 | 1,80 | 25 |
| 5 | 0,50 | 65 | 220 | 2,50 | 30 |

Экспериментальные исследования показали, что разработанный прототип системы позволяет не только существенно сократить время отклика приложе-

ний и сервисов в сети мультиоблачной платформы при проведении кибератак, но и поддерживать заданное качество обслуживания на требуемом уровне.

В дальнейшем планируется исследовать работу прототипа на предмет ресурсоемкости, а также поведение при различных типах кибератак.

Исследование выполнено при финансовой поддержке РФФИ (проекты 16-37-60086, 16-07-01004, 18-07-01446) и гранта Президента Российской Федерации для государственной поддержки молодых российских ученых - кандидатов наук (МК-1624.2017.9).

*Список литературы*

*1 Болодурина И.П., Парфёнов Д.И. Управление потоками данных в высоконагруженных информационных системах, построенных на базе облачных вычислений [Текст] / И.П. Болодурина, Д.И. Парфёнов // Системы управления и информационные технологии. – 2015. - № 1.1. – С. 111-118.*

*2 Bolodurina I.P., Parfenov D.I. Dynamic routing algorithms and methods for controlling traffic flows of cloud applications and services [Текст] / Bolodurina I.P., Parfenov D.I. // Вестник Южно-Уральского государственного университета. Серия: Вычислительная математика и информатика. – 2017. - Т 6. - № 2. – С. 84-98.*

*3 Пальчевский, Е.В. Разработка системы обнаружения низкоактивного несанкционированного сетевого трафика / Е.В. Пальчевский, А.Р. Халиков // Перспективные информационные технологии. Изд-во: «СНЦ РАН», Самара, 2017. – С. 266-269.*

*4 Rafique M., Chen P., Huygens C., Joosen W. Evolutionary algorithms for classification of malware families through different network behaviors //Proceedings of the 2014 conference on Genetic and evolutionary computation. ACM, 2014. С. 1167–1174.*

*5 Bakhareva N.F., Polezhaev P.N., Ushakov Yu.A., Shukhman A.E. SDN-based firewall implementation for large corporate networks // Proceedings of 2017 IEEE 11th International Conference on Application of Information and Communication Technologies (AICT 2017), 2017. – P. 313-318.*

*6 Частикова, В.А. Обнаружение DDoS-атак на основе нейронных сетей с применением метода роя частиц в качестве алгоритма обучения / В.А. Частикова, К.А. Власов, Д.А. Картамышев // Фундаментальные исследования. № 8-4. Изд-во: «Академия Естествознания», Пенза, 2014. – С. 829-832.*

*7 Коржов, В. Современные DDoS-атаки / В. Коржов // Журнал сетевых решений LAN. № 9. Изд-во: «Открытые системы», Москва, 2016. – С. 55-57.*

*8 Юнг, Й.Ф. Защита от DDoS-атак из облака / Й.Ф. Юнг // Журнал сетевых решений LAN. № 5. Изд-во: «Открытые системы», Москва, 2014. – С. 63-65.*