УДК 004.056, 004.72

БЕЗОПАСНОСТЬ И УСТОЙЧИВОСТЬ СИСТЕМ МОБИЛЬНЫХ ГРАНИЧНЫХ ВЫЧИСЛЕНИЙ

[1]Багрова В.А., [2]Багров А.П.

[1]Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» РТУ МИРЭА, 119454, Россия, г. Москва, Проспект Вернадского, д. 78., e-mail Story_teller@bk.ru

[2]Общество с ограниченной ответственностью "Келли Сервисез ИТ Решения", 129110, Россия, г. Москва, Проспект Мира, 33, корпус 1, e-mail solmayers@yandex.ru

В данной статье рассматриваются вопросы безопасности и устойчивости систем, построенных на основе активно развивающейся технологии - мобильных граничных вычислений. Авторами освещены предпосылки развития технологий «расширенного облака» - туманных и граничных вычислений, представлена структура эталонной системы граничных вычислений. Рассмотрены вопросы безопасности и устойчивости: в первую очередь унаследованные от облачных технологий, затем уникальные для граничных систем. Для решения обозначенных проблем авторы предлагают ряд подходов как организационных, так и технических. В них особое место занимает создание и внедрение подсистемы поиска аномалий. Кроме этого, предложено управление на основе политик или правил разного уровня для подобных комплексных систем.

Ключевые слова: Интернет вещей, граничные вычисления, туманные вычисления, облачные технологии, устойчивость систем, информационная безопасность, стандартизация

SECURITY AND RESILIENCE OF MOBILE EDGE COMPUTING SYSTEMS

[1]Bagrova V.A, [2]Bagrov A.P.

[1]Federal State Educational Institution of Higher Education "MIREA - Russian Technological University" RTU MIREA, 119454, Russia, Moscow, Vernadsky avenue, 78, Story_teller@bk.ru
[2]Limited Liability Company "Kelly Services IT Solutions", 129110, Russia, Moscow, Prospect Mira., 33/1, e-mail solmayers@yandex.ru

This article addresses the issue of security and resilience of systems using an actively developing technology – mobile edge computing. Authors highlight the background for development of "extended cloud" – fog and edge computing. This article also contains reference structure of edge computing system. Security and resilience issues are considered – from those that are inherited from cloud technologies to ones specific for edge computing systems. Authors propose a number of organizational and technical solutions for such problems and issues. Implementation of anomaly detection subsystem is specifically highlighted among them. In addition, authors propose to utilize management based on policies and rules of different levels for corresponding complex systems.

Key words: Internet of things, edge computing, fog computing, cloud technologies, system resilience, information security, standardization

Введение

Облачные вычисления (ОВ) можно назвать определяющей технологией последнего десятилетия, когда речь заходит о хранении и обработке больших объемов информации. В основе архитектурной концепции облачных вычислений лежит использование центров обработки данных (ЦОД), связанных друг с другом при помощи оптических сетей и образующих, соответственно, единую сеть, позволяющую осуществлять обмен данными между ЦОДами с низкими задержками. Такие выгодные особенности облачных вычислений, как самообслуживание по требованию, универсальный сетевой доступ, объединение ресурсов, мгновенная масштабируемость и измеряемый сервис поддерживают востребованность облачных систем.

За прошедшие годы масштаб распространения облачных технологий значительно увеличился. Мировые крупнейшие компании, в числе которых Google, Amazon, Ebay, инвестируют значительные капиталы в развитие и использование облачных вычислений, а многие другие организации стоят перед неизбежной необходимостью

внедрять облачные технологии в свои бизнес-процессы. Согласно выпущенному в начале 2018 года седьмому ежегодному отчету Cisco Global Cloud Index 2016-2021 ("Глобальный индекс развития облачных технологий в период с 2016 по 2021 гг."), был зафиксирован крайне быстрый (в 1.5 раза) рост трафика ЦОД. Такой прогресс связывают в том числе с совершенствованием методов контроля и безопасности облаков, а также с развитием Интернета вещей.

Рис.1 – Рост рынка HyperScale дата центров [1].

Тенденция к развитию интернета вещей способствовала выявлению новых требований к облачным вычислениям. Крупные дата-центры, расположенные в разных частях мира, действительно обладают мощностью, способной обработать запросы очень большого количества пользователей. Однако часто они находятся физически далеко от пользователя, и это отражается на скорости, с которой конечное устройство обменивается информацией со своим облаком, порой приводит к задержкам и явлению неустойчивости синхронизации. Результатом решения этих проблем стало появление новых технологий, способных удовлетворить поставленные требования.

Новыми технологиями стали туманные и мобильные граничные вычисления. Эти технологии представляют собой так называемое «расширенное облако» (extended cloud) и позволяют производить вычисления ближе к источнику данных. Сокращение физического расстояния предполагает повышение качества предоставляемых услуг благодаря уменьшению задержки между сервером и конечными узлами.

Концепции туманных и граничных вычислений являются близкими, но, тем не менее, имеют отличия в методах обработки и передачи данных. Каждая из них имеет преимущества и недостатки. Граничные вычисления (ГВ) предполагают обработку данных прямо на периферии сети, очень близко к источнику данных, что приводит к крайне низкому уровню задержек. В сети туманных вычислений собранные данные отправляют на обработку в узел сети (fog node), расположенный близко к области сбора. Туманные вычисления предполагают централизованную обработку данных и являются, за счет этого, более масштабируемой технологией, однако по скорости реагирования отстают от граничных.

В первую очередь в статье будет рассмотрена эталонная архитектура граничных вычислений. Это позволит получить представление о подобных системах и элементах, которые их образуют. Затем обозначены текущие проблемы граничных вычислений и предложен ряд имеющихся и разрабатывающихся решений в этой области.

1. Архитектура граничных вычислений

Европейский институт по стандартизации в области телекоммуникаций выпустил стандарт ETSI GS MEC 003 V1.1.1 (2016-03), определяющий структуру и архитектуру систем, построенных на основе мобильных граничных вычислений.

На рисунке 2 представлена эталонная архитектура системы мобильных граничных вычислений, включающая функциональные элементы, из которых состоит система, и контрольные точки трех видов:

связанные с платформой МГВ (Mp), связанные с управлением ГВ (Mm) и связанные с внешними элементами (Mx). Уровень хоста представлен самим хостом (конечным узлом сети) и объектами управления хостом. Хост ГВ состоит из платформы ГВ и инфраструктуры виртуализации, которая обеспечивает вычислительные, сетевые ресурсы, а также ресурсы для хранения данных.

Платформа граничных вычислений содержит набор необходимых функций, необходимых для запуска приложений в конкретной инфраструктуре виртуализации, и позволяет приложениям предоставлять и потреблять периферийные службы.

Элементы управления хостом включают диспетчер платформы граничных вычислений и диспетчер инфраструктуры виртуализации и обеспечивает управление хоста с учетом приложений, запущенных на нем.

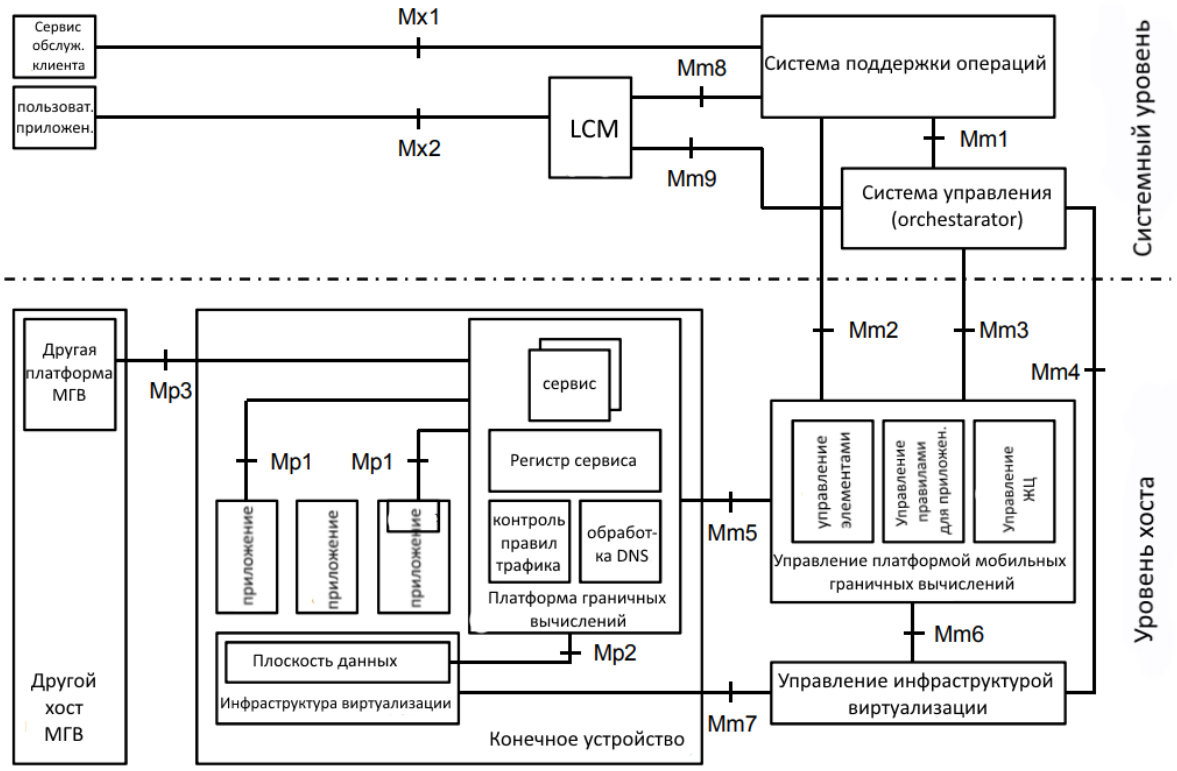

Рис.2. Архитектура и контрольные точки системы граничных вычислений [2]

На системном уровне элементы управления представлены оркестратором в качестве основного компонента, который контролирует всю систему. Система поддержки операций получает запрос от конечного пользователя или от сервиса обслуживания об отключении или подключении приложений и передает эти команды оркестратору.

2. Проблемы, наследуемые от классической облачной структуры

Переход к облачной инфраструктуре не только приносит пользу для бизнеса, но и приводит к ряду новых проблем, характерных исключительно для облака. В облачной среде конечные пользователи имеют гораздо меньше контроля над оборудованием, программным обеспечением и данным. В сочетании с невысоким уровнем «прозрачности» процессов в облаке это приводит к проблемам в сфере безопасности и росту неопределенности для организаций.

Злоумышленники тоже заметили рост популярности облаков, и в 2017 году количество атак на облака выросло на 300%, согласно Global Security Intelligence Report от Microsoft[3].

Недоступность облачных сервисов и их сбои приводят к расходам со стороны компаний. Согласно отчёту от Lloyd's of London and the American Institutes for Research [4], недоступность хотя бы одного из основных поставщиков облачных решений в США в течении 3-6 дней приведёт к потере более чем 19 миллиардов долларов со стороны крупного и среднего бизнеса, и только 1.1-3.5 миллиарда долларов из этой суммы могут быть теоретически покрыты страховками.

Помимо требований безопасности, вызванных вышеназванными рисками, системы мобильных граничных вычислений наследуют также требования к устойчивости от облачной инфраструктуры.

Устойчивость определяется как способность системы обеспечить допустимый уровень услуг при наличии проблем или сбоев [5]. Устойчивость системы является количественной характеристикой, однако не существует общепризнанной методологии ее измерения в данном контексте. Часть из существующих подходов рассмотрены в работе [5]. Подробное рассмотрение вопросов измерения устойчивости выходит за рамки этой статьи.

Допустимый уровень услуг определяется конечным клиентом и обычно закрепляется в соответствующих юридических документах. Кроме допустимого уровня услуг существуют еще несколько метрик, которые зависят от особенностей поставляемых услуг. RTO – целевое время восстановления и RPO – целевая точка восстановления.

RTO является показателем того промежутка времени, в течении которого система должна быть восстановлена после нарушения работы сервиса. RPO – это ближайшая временная точка состояния системы, к которой требуется восстановление.

Устойчивость касается не только доступности сервисов, но даже конфиденциальности и целостности данных в случае инцидентов. Стандартные решения для повышения устойчивости систем требуют доработки с учётом свойств, которыми обладают облачные системы - эластичности, виртуализации, масштабируемости и распределённого физического оборудования.

Вопросы устойчивости зачастую решаются при помощи дублирования: дополнительных устройств хранения для резервных копий, дополнительных линий связи. В облаке нагрузка со стороны клиентов является динамической, и, с учётом эластичности облака, распределение ресурсов и их доступность постоянно изменяются. Это значительно усложняет составление статистической картины и определение требуемых «запасов устойчивости» сервиса.

Поставщики услуг вынуждены устанавливать различные уровни приоритета для приложений в облаке, чтобы предоставлять каждому типу клиентов соответствующие их нуждам метрики и гарантии доступности.

Виртуализация тоже привносит новые риски сбоев и угрозы. Сложные взаимодействия между разными приложениями, сервисами и иной нагрузкой на общем физическом оборудовании усложняет расчёты этих взаимодействий. Расчёты нагрузки и поведения приложений в этих условиях является одним из основных сложных задач данной области.

Распределение физического оборудования в облачной инфраструктуре привносит новые зависимости, что усложняет выполнение соглашений об уровне предоставления услуги (SLA). Кроме этого, здесь могут появиться проблемы с юридической стороны, учитывая законодательство различных стран о хранении определенных типов данных или об ограничении трансграничной передачи определенных категорий информации.

3. Специфика вопроса безопасности и устойчивости граничных вычислений

Кроме классических проблем безопасности, мобильные граничные вычисления имеют свои специфику в этом вопросе.

В условиях граничной инфраструктуры виртуализация охватывает не только дата-центры, но и граничные ячейки. Подобное расширение еще больше уменьшает контроль над устройствами и данными для конечных пользователей.

Одним из преимуществ граничных систем является более высокий процент использования физических ресурсов – уменьшение простоя системы благодаря консолидации рабочих нагрузок. Это преимущество несёт и дополнительные риски. При более высоком проценте использования ресурсов система более подвержена отказам в случае скачков нагрузки или сбоев самого оборудования или сетей.

Кроме этого, возникают дополнительные вопросы взаимодействия и адаптивности систем т.к. значительно увеличивается уровень неоднородности внутри системы. Причем одно приложение может использовать ресурсы сразу нескольких неоднородных платформ, и качество услуг будет зависеть в том числе и от самих приложений на этих платформах, что может привести к дополнительным рискам безопасности и рискам отличий поведения системы от ожидаемого. Подобное расширение потенциально может увеличить в том числе время реагирования на инциденты, в связи с неоднородностью систем и конфигураций.

Поставщикам услуг приходится учитывать и особенности мобильных сетей связи, включая зоны покрытия и стабильность соединения.

Для структурирования конкретных угроз необходимо начать с угроз самой инфраструктуре. Инфраструктура граничной системы является частью «сети последней мили» и использует гораздо больше технологий, чем классические сети, причем каждая из технологий подвержена своим уникальным рискам.

Атаки отказа в обслуживании (DDOS) и глушение сигнала сети могут достаточно легко занять большую часть полосы пропускания и ресурсов конечных устройств.

Атаки «злоумышленник в середине» (Man in the Middle) являются еще одним примером – они могут быть использованы для кражи данных и конфиденциальной информации с различных конечных устройств или в точках связи граничной сети с основным облаком в целом. Подобная инфраструктура также подвержена иным атакам, характерным для мобильной сети.

Классические атаки и угрозы виртуализации актуальны и для граничных систем, с учётом особенностей распределения ресурсов.

Атаки отказа в обслуживании на виртуализацию могут быть еще более актуальны с учётом малых вычислительных мощностей конечных устройств. В таких атаках одна или несколько заражённых виртуальных машин могут занять большую часть полосы пропускания или вычислительной мощности конечного устройства. Заражённые виртуальные машины могут быть использованы для кражи данных или нарушения работы всей системы в целом, с учётом ограниченной полосы пропускания самой сети.

Уровень риска утечки данных зависит от типа системы и классификации данных, что обрабатывает данная граничная инфраструктура. Обычно такая система хранит данные только о локальных пользователей в каждом отдельно взятом окружении, но это усугубляется конфиденциальностью таких персональных данных.

4. Предлагаемые решения

Наличие граничной инфраструктуры должно минимально влиять на доступность сети в целом. Поставщик услуг, как и в случае с облачными решениями, должен предлагать гибкий уровень устойчивости и рассчитывать ресурсы с точки зрения требований клиентов и их приложений.

В случае инцидентов необходим не просто механизм устойчивости, но и механизм обнаружения инцидента и уменьшения его влияния на всю сеть и инфраструктуру. Это требует от поставщика услуг конкретных механизмов обнаружения проблем, специфичных для граничной системы – включая обнаружение проблем некорректных настроек или отказа мобильной сети.

Одним из решений этих задач может стать система обнаружения аномалий. Поставщику услуг необходимо определить нормальное поведение системы и какие отклонения от нормы должны считаться аномалией.

Обнаружение аномалий было рассмотрено для большого количества сфер и приложений [8].

Для инфраструктур, рассматриваемых в данной статье, на данный момент подобные механизмы только развиваются и имеют целый ряд трудностей.

Например, в случае инфраструктуры как сервиса, клиент отвечает за корректную работу своих приложений, в то время как поставщик услуг отвечает только за саму инфраструктуру. Однако, механизм обнаружения аномалий эффективен только в том случае, если сигнал об аномалии приходит с минимальной задержкой и имеет высокую точность. С учётом разделения ответственности, поставщикам услуг будет необходимо встроить в данный механизм разделения аномалий. В некоторых случаях это будет невозможно, т.к. подобное разделение потребует от клиента предоставление доступа поставщику услуг к своим приложениям.

Кроме этого, сама инфраструктура имеет свойство быстро изменять свои паттерны поведения из-за неоднородности физического оборудования и эластичности сервиса. В таких условиях от механизма обнаружения аномалий будет требоваться не только следовать жёстким алгоритмам проверки, но и анализировать ситуацию в реальном времени. Потенциально использование нейронных сетей с большими моделями данных может решить вопрос анализа изменяющегося состояния сети.

Важность обнаружения аномалий в подобных системах исходит из-за зависимости между аномалиями в данных и некорректным поведением системы. Например, аномальные паттерны трафика, исходящего от конечных устройств, могут означать, что резко вырос спрос на данную услугу, что можно считать формой атаки отказа в обслуживании. Повышение нагрузки вне расчётных показателей может привести к деградации сервиса в целом.

Внедрение этой подсистемы напрямую позволяет снизить одну из ключевых метрик управления инцидентами – время обнаружения. Эта величина измеряется как время, прошедшее с начала инцидента до его обнаружения.

Второй ключевой метрикой управления инцидентами является время на решение инцидента, которое определяется как время, прошедшее от обнаружения инцидента до возвращения системы к нормальному состоянию. Подсистема обнаружений аномалий может косвенно снизить эту метрику в зависимости от данных, которые подсистема сможет предоставить владельцу системы граничных вычислений.

Встраивание подобного механизма несёт в себе свои собственные риски, связанные с работоспособностью и масштабируемостью сети. Граничная инфраструктура и её эластичность приводят к необходимости мониторинга в реальном времени, и эта необходимость может изменяться динамически. Основываясь на этих требованиях, система обнаружения аномалий должна обладать не только масштабируемостью, но и потреблять минимальное количество ресурсов на конечных устройствах. Кроме

этого, неоднородность подобной инфраструктуры приводит к необходимости системы обнаружения аномалий работать в различных окружениях и с различным оборудованием одновременно и с минимальными различиями в данных.

Уже известно, что масштабируемость мониторинга возможна [9], однако обнаружение аномалий зачастую происходит после того как данные с мониторинга были сохранены на физическое оборудование. Данный факт приводит к растущим потребностям системы мониторинга в зависимости от масштаба инфраструктуры сети. В работе [10] авторы провели экспериментальный анализ различных методик обнаружения аномалий с учётом эластичности системы. Было обнаружено, что эластичность приводит к уменьшению точности обнаружения аномалий, в том числе затрудняя определение нормального состояния системы со стороны механизма обнаружения аномалий.

Другие исследователи в [11] рассматривают механизм обнаружения аномалий и вторжений с учётом использования агентов на конечных устройствах. Данный подход имеет риски с точки зрения приватности конечных пользователей и повышает требования к конечным устройствам, увеличивая минимальный процент загрузки системы и уменьшая доступные мощности для клиентов.

На данный момент неоднородность каждого решения в сфере граничных систем вызывает необходимость создавать или дорабатывать имеющиеся решения в значительной мере, или принимать риски в сфере безопасности. Другим способом уменьшения рисков может стать уменьшение предлагаемых клиентам ключевых метрик.

Вопросы устойчивости граничной системы близко связаны с вопросами управления и планирования такой системой в целом. Управление, прогнозирование, а главное продажа подобного сервиса зависит от предлагаемых характеристик системы конечным клиентам.

Неоднородность системы, как уже было сказано выше, усложняет планирование нагрузки и вынуждает поставщика услуг предлагать клиентам прогнозы с низкой точностью.

Обычно стратегии и политики управления задают поведение системы. Подобные документы определяются как «ограничения и требования по системе, состоянию системы, переходам состояний и описанием её характеристик» [12].

Граничные системы усложняют составление таких стратегий и документов в связи с быстроизменяющимися состояниями и уменьшенной точностью прогнозов. Использование данных систем требует комплексного подхода и значительного количества обобщений, чтобы свести общее количество состояний системы к конечному числу.

Одним из подходов может являться использование лучших практик из управления комплексными системами – управление на основе политик или правил разного уровня. Ряд специалистов уже предложили платформу для достижения устойчивости в подобных системах [13]. Описанный в исследовании подход может быть применен для граничных систем, но потребует доработки для более неоднородных систем.

Для создания общего подхода к решению проблем безопасности группой Cloud Security Alliance была создана Cloud Controls Matrix [14]. Данный проект предназначен для создания фундаментальных принципов безопасности для различных решений в сфере облачных технологий. Предлагается платформа с учётом иных регуляторных требований, включая ISO 27001/27002, ISACA CoBIT, PCI и NIST.

5. Перспективы развития технологии

В будущем ожидается значительная стандартизация граничной инфраструктуры, что позволит специалистам в области безопасности подойти к вопросу изучения основных рисков и угроз более детально и предоставить набор базовых решений. Уже сейчас появились со стороны ETSI предложения по архитектуре таких систем в сетях 5G [6]

Несмотря на наличие ряда белых книг по вопросам архитектуры, основные вопросы безопасности и устойчивости, поднятые выше, не были рассмотрены в должной мере и, на данный момент, решение данных проблем варьируется в каждом конкретном случае.

Исходя из этого, интеграция механизмов безопасности, устойчивости и приватности должны стать одним из основных направлений развития подобных систем. Другим интересным аспектом может стать объединение граничных систем и виртуализации сетевых функций. ETSI уже рассматривает подобный подход, чтобы в будущем повысить качество услуг от таких систем [7].

Кроме того, на территории Российской Федерации и стран СНГ на данный момент не определен стандарт граничных систем. Развитие нормативной документации и стандартизации этих технологий впоследствии также могло бы способствовать развитию и распространению самой технологии на территории РФ.

Заключение

В данной статье был широко раскрыт вопрос безопасности и устойчивости систем мобильных граничных вычислений. Были освещены предпосылки развития технологий «расширенного облака» - туманных и граничных вычислений, представлена структура эталонной системы граничных вычислений. Далее были рассмотрены вопросы безопасности и устойчивости: в первую очередь унаследованные от облачных технологий, затем уникальные для граничных систем. В качестве решений были предложены стандартизация технологии и, как следствие, внедрение политик и правил на уровне организаций, а также встраивание в граничную сеть системы обнаружения аномалий.

Список литературы

1. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper. // https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html (дата обращения: 9.11.2018)
2. Mobile Edge Computing (MEC); Framework and Reference Architecture. // https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf (дата обращения: 9.11.2018)
3. Global Security Intelligence Report. // https://www.secureworldexpo.com/industry-news/attacks-on-cloud-2017 (дата обращения: 9.11.2018)
4. Cloud down. Impacts on the US Economy. // https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down (дата обращения: 9.11.2018)
5. J. P. Sterbenz, D. Hutchison, E. K. Cetinkaya, A. Jabbar, J. P. Rohrer, M. Scholler, and P. Smith, “Resilience and survivability ¨ in communication networks: Strategies, principles, and survey of disciplines// 2010 Computer Networks, vol. 54, no. 8, pp. 1245–1265
6. MEC in 5G networks. // https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf (дата обращения: 9.11.2018)
7. Mobile Edge Computing -A key technology towards 5G. // https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf (дата обращения: 9.11.2018)
8. Survey on Anomaly Detection using Data Mining Techniques. // https://www.sciencedirect.com/science/article/pii/S1877050915023479 (дата обращения: 9.11.2018)
9. A Scalable Architecture for Network Traffic Monitoring and Analysis // https://www.researchgate.net/publication/220099360_A_Scalable_Architecture_for_Network_Traffic_Monitoring_and_Analysis_Using_Free_Open_Source_Software (дата обращения: 9.11.2018)
10. S. N. Shirazi, S. Simpson, A. Marnerides, M. Watson, A. Mauthe, and D. Hutchison, “Assessing the impact of intra-cloud live migration on anomaly detection,” in Cloud Networking (CloudNet)// 2014 IEEE 3rd International Conference on, Oct 2014, pp. 52–57

a. V. Dastjerdi, K. A. Bakar, and S. G. H. Tabatabaei, “Distributed intrusion detection in clouds using mobile agents,” // 2009 ADVCOMP’09. Third International Conference on. IEEE, pp. 175–180.

b. Goh, A Generic Approach to Policy Description in System Management. // Hewlett Packard Laboratories 1997.

11. A framework for resilience management in the cloud // https://link.springer.com/article/10.1007/s00502-015-0290-9 (дата обращения: 9.11.2018)
12. Cloud Controls Matrix URL : https://cloudsecurityalliance.org/group/cloud-controls-matrix/ (дата обращения: 9.11.2018)

References

1. Cisco Global Cloud Index: Forecast and Methodology, 2016–2021 White Paper. // https://www.cisco.com/c/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.html (accessed: 9.11.2018)
2. Mobile Edge Computing (MEC); Framework and Reference Architecture. // https://www.etsi.org/deliver/etsi_gs/MEC/001_099/003/01.01.01_60/gs_MEC003v010101p.pdf (accessed: 9.11.2018)
3. Global Security Intelligence Report. // https://www.secureworldexpo.com/industry-news/attacks-on-cloud-2017 (accessed: 9.11.2018)

4. Cloud down. Impacts on the US Economy. // https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down (accessed: 9.11.2018)

5. J. P. Sterbenz, D. Hutchison, E. K. C¸ etinkaya, A. Jabbar, J. P. Rohrer, M. Scholler, and P. Smith, "Resilience and survivability ¨ in communication networks: Strategies, principles, and survey of disciplines// 2010 Computer Networks, vol. 54, no. 8, pp. 1245–1265

6. MEC in 5G networks. // https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp28_mec_in_5G_FINAL.pdf (accessed: 9.11.2018)

7. Mobile Edge Computing -A key technology towards 5G. // https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp11_mec_a_key_technology_towards_5g.pdf (accessed: 9.11.2018)

8. Survey on Anomaly Detection using Data Mining Techniques. // https://www.sciencedirect.com/science/article/pii/S1877050915023479 (accessed: 9.11.2018)

9. A Scalable Architecture for Network Traffic Monitoring and Analysis // https://www.researchgate.net/publication/220099360_A_Scalable_Architecture_for_Network_Traffic_Monitoring_and_Analysis_Using_Free_Open_Source_Software (accessed: 9.11.2018)

10. S. N. Shirazi, S. Simpson, A. Marnerides, M. Watson, A. Mauthe, and D. Hutchison, "Assessing the impact of intra-cloud live migration on anomaly detection," in Cloud Networking (CloudNet)// 2014 IEEE 3rd International Conference on, Oct 2014, pp. 52–57

11. A. V. Dastjerdi, K. A. Bakar, and S. G. H. Tabatabaei, "Distributed intrusion detection in clouds using mobile agents," // 2009 ADVCOMP'09. Third International Conference on. IEEE, pp. 175–180.

12. C. Goh, A Generic Approach to Policy Description in System Management. // Hewlett Packard Laboratories 1997.

13. A framework for resilience management in the cloud // https://link.springer.com/article/10.1007/s00502-015-0290-9 (accessed: 9.11.2018)

14. Cloud Controls Matrix URL : https://cloudsecurityalliance.org/group/cloud-controls-matrix/ (accessed: 9.11.2018)