УДК 004.056.55

ХАКЕРСКИЕ КИБЕРАТАКИ В РЕАЛЬНЫХ ОБЛАСТЯХ

Назаров А.Н., Андрианова Е.Г.

МИРЭА - Российский технологический университет, 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: a.nazarov06@bk.ru, dtghmflysq@gmail.com

Показана актуальность необходимости разработки моделей и методов исследования хакерских кибератак как облачных систем класса IaaS, используемых внешне для вполне легальных целей. По результатам проведённого анализа структуры хакерских кибератак, моделей расчётного обоснования ресурсного обеспечения и развёртывания как IaaS, так и сервисов IaaS постановлена и формализована научная задача оценки числа виртуальных соединений IaaS в интересах мониторинга идентификации хакерских кибератак. По результатам решения задачи получена новая оптимизационная модель системы "источники информации различных категорий контента – фрагмент IaaS" . Развит метод покрывающих областей, для расчёта общего количества виртуальных соединений IaaS. Полученные научные результаты могут быть положены в основу автоматизации расчётного обоснования многовариантных проектных решений IaaS на предпроектной стадии.

Ключевые слова: модель, облачные вычисления, IaaS, Система уравнений, подход, неравенство, показатель, метод, сходимость, невырожденность, оптимизация, бот-кибератака, мониторинг, облачный кластер.

HACKING CYBER ATTACKS IN REAL AREAS

Nazarov A.N., Andrianova E.G.

MIREA - Russian Technological University, 119454, Moscow, 78 Vernadsky Avenue, *Russia, e-mail: a.nazarov06@bk.ru, dtghmflysq@gmail.com*

The urgency of the need to develop models and research methods for bot-cyber-attacks as IaaS-class cloud systems used externally for quite legal purposes is shown. The results of the analysis of the structure of botnets, cyberattacks, and models of computational substantiation of resource provision and deployment, both IaaS and IaaS services it was determined and formalized scientific problem of estimating the number of virtual connections IaaS in the interests of monitoring and identification of botnets, cyber-attacks, the results of which received a new optimization model of the system "sources of information different categories of content – fragment IaaS" . The method of covering areas has been developed for calculating the total number of IaaS virtual connections. The obtained scientific results can be used as the basis for automating the computational justification of multi-variant IaaS design solutions at the pre-project stage.

Keywords: model, cloud computing, IaaS, system of equations, approach, inequality, indicator, method, convergence, nondegeneration.

Введение

Массовое применение новых технических средств и информационных технологий, составляющих основу бурно развивающегося процесса информатизации, изменяет образ жизни миллионов людей. Под воздействием информационных технологий меняются формы экономической деятельности. Возникают новые формы общения как профессионального, так и личного.

Цифровая трансформация всех видов деятельности обуславливает расширение спектра и номенклатуры средств проведения бизнес-операций в интересах рыночного первенства.

Компании не только изменяют работу своих функций, но и переопределяют, как взаимодействуют функции и расширяют границы бизнеса. Три строительных блока трансформации бизнес-модели – это изменения в бизнесе на основе цифровизации, создание новых цифровых предприятий и цифровая глобализация [1].

Например, компания «Рив Гош» автоматизировала программу лояльности и маркетинга на базе CRM и BI-решений. Проект охватил более 220 магазинов по всей России и несколько миллионов активных дисконтных карт [2].

Система поддержки лояльности и маркетинга позволила сети «Рив Гош» широко использовать разнообразные скидки и схемы начисления бонусов, среди которых динамические матрицы скидок, продуктовые акции, скидки по целевым магазинам, по купонам, начисление подарочных баллов, оплата баллами, скидки для конкретных групп клиентов.

У службы маркетинга появилась возможность сегментировать клиентскую базу для формирования целевых маркетинговых предложений.

В результате количество проводимых маркетинговых кампаний увеличилось в 15 раз [1]. Сотрудники сервисного и контактного центров теперь могут получить всю информацию о покупателе в едином окне.

Реализация сценария интересов злоумышленника, например, на основе соответствующей DDoS-атаки может оказать весьма серьёзное влияние на интересы большого количества физических лиц – покупателей товаров компании «Рив Гош».

Компании находят способы дополнить свой традиционный бизнес созданием цифровых предложений и цифровых ресурсов, что создаёт предпосылки агрессивных кибератак «на плечах» цифровых ресурсов IaaS самого предприятия.

Причём объектом риска может быть, как само предприятие, так и его клиент. Таким образом, IaaS предприятия становится технологической средой проведения кибератак.

В настоящее время на глобальных рынках наблюдаются устойчивые технологические тренды, которые принято называть «цифровыми» [3]. В таблице приводятся данные Top-10 технологических трендов, выделенных в исследованиях компании Gartner за 2017 и 2019 годы [4,5].

Таблица. Глобальные технологические тренды

	2017	2019
1	ИИ и глубинное машинное обучение	Автономные объекты
2	Интеллектуальные приложения	Дополненная аналитика
3	«Умные вещи»	Разработка приложений на основе ИИ
4	Виртуальная (VR) и дополненная (AR) реальность	Цифровые двойники
5	Цифровые двойники	Усиление периферии
6	Блокчейн и распределённые реестры	Технологии погружения
7	Диалоговые системы	Блокчейн
8	Сетевые приложения и сетевая архитектура	Умные пространства
9	Цифровые технологические платформы	Цифровая этика и приватность
10	Адаптивная архитектура безопасности	Квантовые компьютеры

Как видно из таблицы, глобальное развитие отдельных цифровых технологий носит поступательный характер и происходит в сторону создания сложных цифровых систем, компоненты которых дополняют и взаимодействуют друг с другом. Например, «умные вещи», объединённые с цифровыми двойниками, эволюционируют в автономные объекты и «умные пространства». Диалоговые системы становятся необходимой компонентой приложений машинного интеллекта и т.д.

Важным моментом цифрового бизнеса является не только ожидаемый экономический эффект, но и фактические бизнес-результаты многих компаний. По данным исследований Huawei и Oxford Economics за 2017-2018гг. возврат инвестиций, вложенных в цифровые инструменты, в 6,7 раз выше, чем в «нецифровые, а каждый потраченный на цифровые инструменты доллар добавляет к ВВП страны в среднем $20 [6].

Злоумышленники учитывают современные инновационные тренды для совершенствования своей преступной деятельности в организации новых кибератак. Поскольку IaaS становится базовой технологией, то кибератаки должны учитывать этот факт.

За последние 20 лет все серьёзные кибератаки стали бот-кибератаками. Осознание этой проблемы проявляется в появлении документов международных организаций, координирующих вопросы информационной безопасности. Так, например, Международный союз электросвязи (ITU), на регулярной основе [7], готовит рекомендации и другие документы по этой проблеме.

Известно определение [8] ботнет — это сеть заражённых компьютеров, то есть компьютеров, превращенных в роботов (bot), находящихся под внешним управлением или под управлением зловредного программного кода, внедрённого в систему тем или иным способом.

Таким образом, вся технология создания первых ботнетов состояла в следующем: необходимо было каким-то образом внедрить в клиентский компьютер вредоносный код.

Основу этого кода составлял софт, позволяющий злоумышленнику – бот-мастеру -удалённо управлять чужим компьютером: скачивать с него любые файлы, загружать и запускать программы, редактировать реестр. Такой софт предоставлял бот-мастеру – хозяину ботнет сети, возможность открывать «заднюю калитку» (Backdoor) в клиентском компьютере. После чего этот код при каждом сеансе связи подключал заражённую машину к некой IRC-сети (Internet Relay Chat), а бот-мастер этой сети «видел» все включённые в неё клиентские компьютеры. Соответственно бот-мастер через установленный IRC-канал мог посылать заражённым клиентским компьютерам

— их стали называть зомби-машинами — команды, причём как всем зомби сразу, так и каждому в отдельности.

Лавинообразный рост применимости web-технологий, как средства инновационных решений для различных областей человеческой деятельности, является фактором развития мировой эволюции. Эволюция же ботнетов к настоящему времени привела к появлению гибридных ботнетов, принципиально работающих на web-технологиях и вобравших в себя функциональные возможности ранее созданных ботнетов.

Гибридный ботнет, схематично изображён на рис.1 [8]. Использует команды как минимум двух протоколов. Характеристики гибридного ботнета заключаются в следующем:

- гибридный ботнет использует несколько серверов C & C (Command&Control) и их всех синхронизирует;
- если один C & C сервер заблокирован, то команды могут быть доставлены в зомби через другие серверы C & C. Таким образом, чтобы решить проблемы ботнетов, каждый C & C сервер должен быть заблокирован;
- только сервент-боты1 из списка выбранных бот-мастером узлов могут действовать как сервер C & C и использовать публичный IP адрес. Также сервент-бот может, обычно случайным способом, выбирать номер коммуникационного порта, например, номер порта 22 (SSH), или 443 (HTTPS);
- C & C сервер может создавать личный / открытый ключ, затем использовать его при направлении команд атаки.
- гибридные ботнеты обычно используют P2P протокол для синхронизации C & C серверов или IRC (Internet Relay Chat). Возможно использование протокола HTTP для связи между зомби.

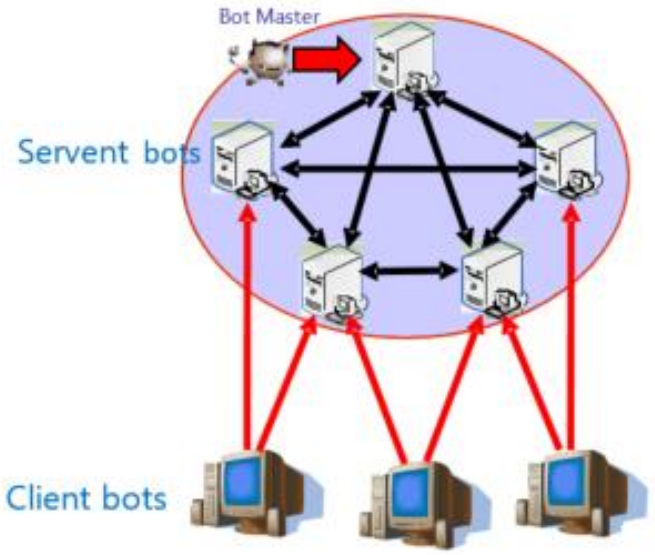

Рис. 1. Схема гибридного ботнета

Web-ориентированные ботнеты отличаются тем, что управление ими не обязательно осуществлять через компьютер как таковой. Для доступа к web-ориентированным ботнетам годится любое мобильное устройство с выходом в Интернет.

Постановка задачи

Основным понятием архитектуры «облачной» модели, является «Сервис». Не претендуя на полноту определения этого понятия будем считать, что это программный комплекс системы, реализующий законченную функцию (или несколько функций) по обработке и предоставлению данных [9]. При этом «оказанная услуга» - это выполненные в интересах пользователя функции или предоставленные ему ресурсы по договору.

Инфраструктура как услуга (IaaS – Infrasructure as a service) – это облачная услуга, когда пользователю предоставляется вычислительная инфраструктура виртуальной платформы, которую он самостоятельно настраивает [9]. Потребительские возможности IaaS весьма разнообразны и широки. А с развитием Интернета-вещей и практической реализацией подходов Искусственного интеллекта спектр возможного применения IaaS постоянно расширяется.

[1] Сервент-бот – сервер, который может выполнять функции C&C сервера, по команде бот-мастера

Структурно Облачные вычисления состоят из внешней и внутренней компонент [10]. Эти два компонента связаны через Интернет. С помощью внешней части пользователь взаимодействует с системой, а внутренний компонент – это само облако. Внешний компонент состоит из терминалов пользователей или локальной сети предприятия, а также приложений, используемых для доступа к облакам. Внутренний компонент состоит и з предоставляемых пользователям приложений, серверов, хранилищ данных и других элементов облака.

Архитектуре облачных вычислений посвящены рекомендации ITU-T [11-14]. Общие положения функциональной архитектуры описаны в рамках рекомендации [11].

В общем случае функциональная архитектура Облачных вычислений представляется в виде многослойной модели, в которой конкретные типы функций сгруппированы по слоям, и где имеются интерфейсы между функциональными компонентами в последовательных слоях [10].

Бот-кибератаки в отношении объектов риска суть принадлежащих Iaas реализуются с учетом технологических особенностей виртуализации. Как и любой сервис, они должны использовать виртуальные соединения (ВС) в процессе нанесения ущерба и использовать инфраструктурные особенности IaaS.

Облачный кластер системы мониторинга [15] бот-кибератак может отслеживать состояния всех виртуальных соединений конкретной IaaS , для своевременной идентификации начала бот-кибератаки.

В настоящее время отсутствуют универсальные методические подходы разработки моделей расчётного обоснования виртуальных соединений IaaS и расчётного обоснования проектных решений для облачных экосистем этого класса для различных предметных областей, что предопределяет неотложную необходимость проведения исследований по упомянутой проблематике, что и будет отражено в настоящей статье.

Возможности существующих моделей и методов расчета IaaS

Широкий диапазон скоростей передачи – от нескольких сот бит/с до сотен Мбит/с, существенный статистический характер информационных потоков, большое разнообразие сетевых конфигураций – все эти факторы значительно усложняют описание трафика в современных облачных системах по сравнению с классическими сетями связи [16].

Результат ступенчатой аппроксимации полипачечного случайного процесса $\tilde{b}_d^{(s)}(t)$ битовой скорости трафика контента s-го источника в IaaS на множестве временных пачечных интервалах $\left\{\left[t_{o_j}^{(s)}, t_{p_j}^{(s)}\right]\right\}_{j=1}^{n_s(t)}$ к моменту t текущей сессии есть [16-19]

$$\tilde{b}_d^{(s)}(t)=\sum_{i=1}^{n_s(t)} B_{max_i}^{(s)}\left[\Theta\left(t-t_{o_i}\right)-\Theta\left(t-t_{p_i}\right)\right], \qquad (1)$$

а функция распределения вероятностей этого случайного процесса [19]

$$F_t\left(\tilde{b}_d^{(s)}\right)=\sum_{i=1}^{n_s(t)} p_i^{(s)}\left[\Theta\left(t-t_{o_i}\right)-\Theta\left(t-t_{p_i}\right)\right]\Theta\left(\tilde{b}_d^{(s)}-B_{max_i}^{(s)}\right),$$

где $p_j^{(s)}$ вероятность того, что $\tilde{b}_d^{(s)}(t)$ принимает значение $B_{max_j}^{(s)}$,

$\Theta(t)=\begin{cases}0, t<0,\\ 1, t\geq 0,\end{cases}$; а $\sum_{j=1}^{n_s(t)} p_j^{(s)} k_{B_j}^{(s)}=1$ – характеристическое свойство, $\left\{k_{B_j}^{(s)}\right\}_{j=1}^{n_s(t)}$ –конечное множество коэффициентов пачечности.

Свойство пачечности модели (1) позволило разработать метод статистического уплотнения передачи и обработки группового трафика [19], что является основой повышения эффективности использования ресурсов в сетевых и узловых фрагментах IaaS.

Данная модель трафика контента IaaS была положена в основу [16] разработки модели ресурсного обеспечения IaaS, которая сводится к решению задачи условной оптимизации IaaS.

В результате решения такой задачи условной оптимизации IaaS в пределах выделенных финансовых средств будет получена оценка распределения по узлам IaaS информационно-телекоммуникационных средств (оборудования), ресурсов и решаемых задач. Решение позволяет определить, при необходимости, необходимые инвестиции в проектные решения IaaS с оптимизацией информационных потоков.

На практике, после проведения расчётного обоснования на модели, выделенные задачи должны быть подвергнуты процедуре автоматизированного проектирования для создания эффективных подсистем IaaS на принципах модульности и типизации. Полученные цифровые кластеры можно будет считать цифровыми

платформами IaaS.

Разработанная на основе энтропийного подхода модель системы «источники информации - граничные узлы» IaaS [16] описывает наиболее вероятное распределение ВС от источников информации по фиксированным в пространстве граничным узлам IaaS, и все её коэффициенты имеют определённый физический смысл. Модель позволяет получать значения верхней и нижней оценок числа ВС как функций значений битовой скорости информационных источников.

Предложено [16] развитие метода покрывающих областей для решения задачи расчёта числа виртуальных соединений внутри пространства IaaS. Новый алгоритм этого метода позволяет реализовать пошаговую процедуру расчёта числа виртуальных соединений в IaaS на основе направленного формирования покрывающих областей сгущения трафика, базирующегося на энтропийном подходе.

По завершении расчётов имеем план распределения ВС от всех источников поставки контента по всем фрагментам IaaS.

Остаётся открытым вопрос о том, сколько ВС трафика различных категорий контента можно разместить в телекоммуникационном (звено) или узловом (сервер, Дата центр, хост и т.п.) фрагменте IaaS. Ответ на этот вопрос поможет проектировщикам, сетевым администраторам и исследователям рассчитывать потребную производительность узлов и пропускную способность звеньев IaaS, а также обосновывать структурно-топологическую конфигурацию и архитектурные особенности IaaS, включая ресурсное обеспечение и абонентскую емкость различных сервисов.

Формулировка задачи расчёта числа виртуальных соединений для доставки контента разных категорий во фрагменте IaaS

Для решения задач обеспечения все возрастающего количества потребностей пользователей сервисов IaaS из различных предметных областей поставщики сервисов используют разные источники трафика различных категорий контента с разными требованиями QoS. Это может быть контент для решения логистических задач, телемедицинских услуг и др.

Эпидемия короновируса обусловила повсеместное введение режима самоизоляции, что привела к насущной необходимости реализации сервисов телеконференций и дистанционной обработки в таких сферах человеческой деятельности, как образование, ритейл, проведении совещаний и др.

Вероятностно-временные и другие тактико-технические характеристики, формирующие требования QoS, по доставке контента в фрагменте IaaS обуславливают различные категории контента.

Например, различают следующие основные категории (классы) трафика:

A – трафик, создаваемый источником, передающим информацию с постоянной скоростью (Constant Bit Rate – CBR);

B и C – трафики, создаваемые источником, передающим информацию с переменной битовой скоростью (Variable Bit Rate) соответственно в реальном времени (real time VBR) и не в реальном времени (non-real time VBR);

D, разделяющаяся на две подгруппы (подкласса) – трафик на доступной битовой скорости (Available Bit Rate – ABR) и трафик на неспецифицированной (неопределённой битовой скорости передачи (Unspecified Bit Rate – UBR).

Расчёт B_{need} –требуемого значения ресурса в фрагменте IaaS для реализации всех n категорий сервисов для всех m арендаторов в текущий момент времени t можно осуществить с использованием методических рекомендаций [15-18].

Обозначим B_i^j суммарную битовую скорость трафика j-го арендатора по всем i-м категориям контента во фрагменте IaaS в текущий момент времени t.

Тогда выполняется условие

$$\sum_{j=1}^{m} B_i^j = b_i,\ i=1,2,\ldots,n.$$

Пусть в этом же фрагменте IaaS - $b_i = const_i,\ i \in I = \{1,2,\ldots,n\}$– ресурсы, необходимые для качественного обслуживания всех n категорий контента соответственно в данный момент времени t.

Тогда B_{need} можно распределить между всеми n категориями контента по следующему способу:

$$\left.\begin{array}{c} B^1 < b_1 \le B_{need}, \\ B^2 < b_2 \le B_{need} - b_1, \\ B^3 < b_3 \le B_{need} - (b_1 + b_2), \\ \cdots \\ B^n < b_n \le B_{need} - (b_1 + b_2 + \cdots + b_{n-1}). \end{array}\right\} \quad (2)$$

Обозначим через x_{ij} число ВС j-го арендатора i-й категории контента во фрагменте IaaS,

где i=1,2,…,n, $j = \overline{1,m}$.

Матрица $X=\|x_{ij}\|$ называется распределением ВС всех категорий контента между всеми m арендаторами во фрагменте IaaS и характеризует свойства, как этого фрагмента, так и IaaS в целом.

Пусть b_{ij} – текущее усредненное значение групповой битовой скорости (группового ресурса) трафика контента от всех x'_{ij} источников контента i-й категории j-го арендатора по ВС во фрагменте IaaS, определяемое как

$$b_{ij}=\frac{1}{x'_{ij}}\sum_{s=1}^{x'_{ij}} b_{ij}^{(s)}, \quad (3)$$

где $b_{ij}^{(s)}$ определяется с помощью (1).

Тогда справедливы следующие соотношения

$$\sum_{j=1}^{m} x_{ij}b_{ij}=\sum_{j=1}^{m} B_i^j,\ i=1,2,\ldots,n. \quad (4)$$

Заметим, что лучшие инженерные практики проектирования фрагментов IaaS свидетельствуют о целесообразности некоторого завышения значений b_i, например, согласно правилу

$$\prod_{j=1}^{m} \frac{B_i^j}{b_i-\varepsilon_i}=1,\ i=1,2,\ldots,n, \quad (5)$$

где $b_i - B_i^j = \varepsilon_i > 0$, i=1,2,…,n играет роль показателя "неприкосновенного запаса" относительной производительности (ресурса) фрагмента IaaS, выделенного для обслуживания i-ой категории контента и может задаваться как параметр из практических соображений.

Выбор ε_i обусловлен учётом свойств технологий (прежде всего пакетных) фрагмента IaaS, в том числе системы управления IaaS и выполнения других функций.

Логарифмируя (5), получим

$$\sum_{j=1}^{m} lnB_i^j=nln(b_i-\varepsilon_i)= lnb'_i,\ \ i=1,2,\ldots,n.$$

В итоге

$$\sum_{j=1}^{m} lnB_i^j = lnb'_i,\ i=1,2,\ldots,n. \quad (6)$$

Все существенные требования QoS IaaS, представленные в модели, разработанной и исследованной в [15], после соответствующих переобозначений можно записать для фрагмента IaaS в виде

$$\sum_{i=1}^{n}\sum_{j=1}^{m} c_{ij}^l x_{ij}=C^l,\ l = \overline{1,L}, \quad (7)$$

где c_{ij}^l – значение l-го показателя QoS фрагмента IaaS;

C^l – ограничение на l-й показатель QoS IaaS;

L – число ограничений на показатели QoS IaaS, учитываемые в модели.

С учётом того, что число ВС во фрагменте IaaS может быть записано в виде

$$N = \sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij},$$

число состояний IaaS может быть записано в виде

$$W(x)=\frac{N!}{\prod_{ij} x_{ij}!}.$$

Так как рассматривается крупномасштабная территориально-распределённая IaaS, то число источников контента разных категорий велико. С использованием формулы Стирлинга [15] можно записать

$$lnW=lnN! - \sum_{i=1}^{n}\sum_{j=1}^{m} x_{ij}\, lnx_{ij}. \quad (8)$$

Тогда задача поиска матрицы $X=\left\|x_{ij}\right\|$, с которой связано наибольшее число $W(x)$ состояний при ограничениях (4),(6),(7) формально сводится в "энтропийной постановке" [15] к поиску максимума lnW при ограничениях (4),(6),(7). Данная задача условной оптимизации решена с помощью метода неопределенных множителей Лагранжа в [19].

Развитие метода покрывающих областей для решения задачи расчёта числа виртуальных соединений в IaaS

Основываясь на методе [20], предлагается продолжить расчёт по шагам, путём дальнейшего направленного формирования покрывающих областей, пока не будет исчерпано полностью, либо до необходимого предела узловое пространство IaaS, следующим алгоритмическим образом.

1. На каждом шаге, в зависимости от конкретики структурно-топологической физической реализации подключения сетевых трактов (звезда, кольцо, дерево и др.), в направлении интересуемого одного или нескольких информационных тяготений, либо вдоль одного или нескольких виртуальных путей, либо просто "сужением" ("стягивнием") с целью дальнейшего тотального перебора узлового пространства IaaS формируем новые покрывающие области, в которых происходит сгущение трафика. В этих областях сосредоточены ранее рассмотренные граничные узлы IaaS и соединенные с ними посредством сетевых трактов транзитные узлы IaaS.

2. Теперь граничные узлы IaaS выступают в роли соответственно источников и получателей агрегированной информации, транзитные узлы IaaS выступают в роли распределителей агрегированной, статистически уплотненной [20] информации. Покрывающая область теперь является двухполюсником или звеном.

3. После переопределения исходных данных, в том числе по результатам решения на первом шаге системы линейных уравнений [20] либо аналогичной ей на последующих шагах, составляется новая система уравнений, аналогичных (4)–(8). И опять на основе энтропийного подхода формулируется новая задача условной оптимизации, решение которой сводится к системе линейных уравнений, аналогичной [20].

Решение этой системы линейных уравнений позволяет оценить потенциальное максимальное количество ВС внутри рассматриваемой части IaaS, ограниченной новыми покрывающими областями, что также является важной характеристикой всей системы IaaS в целом.

4. Возвращаемся на вышеуказанный п.1, если не перебрали все узлы пространства IaaS до необходимого предела. Иначе, по завершении расчётов имеем план распределения ВС от всех источников и получателей информации по всем фрагментам IaaS.

Если перейти от рассмотрения битовой скорости источника информации (2) к пакетной (ячеечной) скорости

$$r_{cell}^{(s)}(t)=\tilde{b}_d^{(s)}(t)/\left(L_{inf}+L_{head}\right),$$

Где L_{inf}, L_{head} – соответственно длина информационной части и заголовка пакета, то весь вышеизложенный формализм после соответствующих несложных преобразований, можно применять для любых пакетных сетей IaaS, ориентированных на соединение.

Отметим, что во всех рассмотренных выше моделях оптимизации фигурировали ограничения в виде равенств. На практике, при создании систем очень часто используются условия в виде неравенств. Ограничения в виде неравенств сводятся к ограничениям в виде равенств известным способом [20], суть которого заключается в следующем. К искомым переменным добавляются новые фиктивные переменные, которые в других условиях, где они не используются, входят с нулевыми коэффициентами.

Сходимость метода обусловлена конечномерностью пространства IaaS. Скорость сходимости, точность и устойчивость решений впрямую зависит от размерности и значений коэффициентов решаемой на каждом шаге, системы линейных уравнений. При этом обязательно исследование матрицы, составленной из упомянутых коэффициентов, на невырожденность.

Заключение

По результатам анализа направлений инновационного развития современных предприятий показано, что злоумышленники используют облачную IaaS данных предприятий в качестве технологического пространства

проведения бот-кибератак в отношении объектов риска, как самих предприятий, так и их клиентов. Для идентификации и пресечения таких бот-кибератак в мониторинговом облачном кластере необходимо отслеживать виртуальные соединения для передачи контента в интересах всех процессов в IaaS.

При достаточно общих предположениях, обладающих общностью применения, поставлена, сформулирована и решена научная задача отслеживания виртуальных соединений для передачи контента разных категорий IaaS. Решение такой научной задачи сводится к решению задачи условной оптимизации в «энтропийной постановке» по поиску матрицы распределений виртуальных соединений между всеми арендаторами ресурса фрагмента IaaS, которым поставляются разные категории контента и основано на методе неопределённых множителей Лагранжа.

По результатам решения этой задачи условной оптимизации получена оптимизационная модель распределения ВС от источников контента разных категорий по арендаторам сервисов во фрагменте IaaS. Модель сводится к решению полной системы линейных уравнений, и все её коэффициенты имеют определённый физический смысл. Модель позволяет получать значения верхней и нижней оценок числа ВС как функций значений битовой или пакетной скорости источников контента разных категорий.

Определены условия применимости модели, точности и устойчивости решений по оценке числа ВС во фрагменте IaaS.

Полученные в данной работе результаты могут быть полезными при решении задачи создания и развития облачного мониторинга бот-кибер атак в отношении объектов риска IaaS различного назначения.

Список литературы

1. George Westermann, Didier Bonnet, Andrew McAfee. The Nine Elements of Digital Transformation, 07-01-2014 https://www.newgenapps.com/blog/9-elements-of-digital-transformation-that-guide-digitization
2. Сергей Родионов. Цифровая трансформация требует эволюции в трех измерениях https://www.cnews.ru/reviews/retail2018/interviews/sergej_rodionov
3. Kasey Panetta. Gartner Top 10 Strategic Technology Trends for 2019. Gartner study report https://www.gartner.com/en/newsroom/press-releases/2018-10-15-gartner-identifies-the-top-10-strategic-technology-trends-for-2019
4. David Cearley, Mike Walker, Brian Burke. Top 10 Strategic Technology Trends for 2017. Gartner study report. https://ru.scribd.com/document/334235111/Top-10-Strategic-Technology-Trends-for-2017
5. A.Nazarov 2020, ′Artificial Intelligence Methods in information warfare′, paper presented in the Collection of proceedings of XIV International Industry Conference "Information Society Technologies", Russia, Moscow Technical University of Communications and Informatics, The Publishing House Media publisher, March 18-19, 2020, pp. 295-296.
6. Анна Самойдюк. 20 лучших примеров использования ИИ в ритейле. 2019 https://rb.ru/story/ai-in-retail/
7. http://www.itu.int. Recommendation ITU-T X.15000(04/2011) Overview of cybersecurity information Exchange.
8. Nazarov, A 2012, ′Botnet tracking and global threat intelligence -behavior approaches to identifying distributed botnets′, paper presented in the annual Collection of Cybersecurity Summit (WCS), 2012 Third Worldwide, New Dehli, 30-31 Oct. 2012. DOI:10.1109/WCS.2012.6780878, pp.1-5.
9. Shakhmatov, A, Lyamin, A, Borisov, V & Ples, K 2019, ′ On the analysis of requirements to information security in the public "cloud systems"′, paper presented in the Collection of proceedings of XVIII scientific and practical conference "Information technologies in public administration. Digital transformation into human capital", Russia, Moscow, Federal state unitary enterprise "Research Institute "Voskhod", April 25, pp. 67-80.
10. Mekkel, A 2019, ′Cloud computing. Main feature′, paper, presented in the Collection of proceedings of XIII International Industry Conference "Information Society Technologies", Russia, Moscow Technical University of Communications and Informatics, The Publishing House Media publisher, March 20-21, 2019. In 2 volumes, Vol. 2, pp. 58-60.
11. ITU-T, "Information technology – Cloud computing – Reference architecture". Recommendation Y.3502, August 2014.
12. ITU-T, "Functional architecture for Desktop as a Service". Recommendation Y.3504, June 2016.
13. ITU-T, " Cloud computing – Functional architecture for Network as a Service". Recommendation Y.3515, July 2017.
14. ITU-T, " Cloud computing – Functional architecture for intercloud computing". Recommendation Y.3516, September 2017.
15. Nazarov, A., Nazarov, M., Pantiuhin, D, Pokrova, S., & Sychev, A 2015, ′Automation of monitoring processes in

web-based neuro-fuzzy formalism′, T-comm – Telecommunications and Transport, vol. 9, no. 8, pp. 26-33.

16. A.N. Nazarov, Alireza Nik Aein Koupaei, Anshita Dhoot, Asyraf Azlan & Seyed Milad Ranaei Siadat 2020, ′Mathematical Modelling of Infrastructure as a Service′, paper presented in the annual Collection of scientific works of International Scientific Conference "2020 SYSTEMS OF SIGNALS GENERATINGAND PROCESSING IN THE FIELD OF ON BOARD COMMUNICATIONS", (IEEE Conference #48371), Moscow Technical University of Communication and Informatics (MTUCI), Institute of Electrical and Electronics Engineers (IEEE), Media Publisher Ltd, 2020, 7 p. – in press.

17. Nazarov, A 2019, ′Model of parallel processing of tasks in the cloud cluster Hadoop′, paper presented in the Collection of proceedings of XIII International Industry Conference "Information Society Technologies", Russia, Moscow Technical University of Communications and Informatics, The Publishing House Media publisher, March 20-21, 2019. In 2 volumes, Vol. 2, pp.69-71.

18. Grigoriev, V & Nazarov, A 2019, ′Methodological aspects of parallel problem solving in the cloud cluster of cyber-attacks monitoring′, paper presented in the Collection of proceedings of XVIII scientific and practical conference "Information technologies in public administration. Digital transformation into human capital", Russia, Moscow, Federal state unitary enterprise "Research Institute "Voskhod", April 25, pp. 28-32.

19. Nazarov, A 2019, ′Processing streams in a monitoring cluster′, Russian Technological Journal, Vol. 7, № 6, pp. 54-65. https://doi.org/10.32362/2500-316X-2019-7-6-56-67

20. A.N. Nazarov, Pramod Narayan Tripathi, M Asif Hasan & Duong Viet Tung, 2020, ′ Virtual connections for IaaS service tenants′, paper presented in the annual Collection of scientific works of International Scientific Conference «2020 Wave electronics and its application in information and telecommunication systems (WECONF – 2020, IEEE Conference #48837)». Saint Petersburg State University of Aerospace Instrumentation. June 01-05, 2020, 5 p., - in press.

21. Nazarov, A & Sychev, K 2011, Models and methods for calculating the indicators of quality of functioning of the equipment units and structural parameters of the network the next generation networks, 2th edn, LLC Policom, Russia, Krasnoyarsk, 491 p.

References

1. George Westermann, Didier Bonnet, Andrew McAfee. The Nine Elements of Digital Transformation, 07-01-2014 https://www.newgenapps.com/blog/9-elements-of-digital-transformation-that-guide-digitization

2. Sergei Rodionov. Digital transformation requires evolution in three dimensions https://www.cnews.ru/reviews/retail2018/interviews/sergej_rodionov

3. Kasey Panetta. Gartner Top 10 Strategic Technology Trends for 2019. Gartner study report https://www.gartner.com/en/newsroom/press-releases/2018-10-15-gartner-identifies-the-top-10-strategic-technology-trends-for-2019

4. David Cearley, Mike Walker, Brian Burke. Top 10 Strategic Technology Trends for 2017. Gartner study report. https://ru.scribd.com/document/334235111/Top-10-Strategic-Technology-Trends-for-2017

5. A.Nazarov 2020, ′Artificial Intelligence Methods in information warfare′, paper presented in the Collection of proceedings of XIV International Industry Conference "Information Society Technologies", Russia, Moscow Technical University of Communications and Informatics, The Publishing House Media publisher, March 18-19, 2020, pp. 295-296.

6. Anna Samoydyuk. 20 best examples of using AI in retail. 2019 https://rb.ru/story/ai-in-retail/http://www.itu.int. Recommendation ITU-T X.15000(04/2011) Overview of cybersecurity information Exchange.

7. http://www.itu.int. Recommendation ITU-T X.15000(04/2011) Overview of cybersecurity information Exchange.

8. Nazarov, A 2012, ′Botnet tracking and global threat intelligence -behavior approaches to identifying distributed botnets′, paper presented in the annual Collection of Cybersecurity Summit (WCS), 2012 Third Worldwide, New Dehli, 30-31 Oct. 2012. DOI:10.1109/WCS.2012.6780878, pp.1-5.

9. Shakhmatov, A, Lyamin, A, Borisov, V & Ples, K 2019, ′ On the analysis of requirements to information security in the public "cloud systems"′, paper presented in the Collection of proceedings of XVIII scientific and practical conference "Information technologies in public administration. Digital transformation into human capital", Russia, Moscow, Federal state unitary enterprise "Research Institute "Voskhod", April 25, pp. 67-80.

10. Mekkel, A 2019, ′Cloud computing. Main feature′, paper, presented in the Collection of proceedings of XIII International Industry Conference "Information Society Technologies", Russia, Moscow Technical University of Communications and Informatics, The Publishing House Media publisher, March 20-21, 2019. In 2 volumes, Vol. 2, pp. 58-60.

11. ITU-T, "Information technology – Cloud computing – Reference architecture". Recommendation Y.3502, August 2014.

12. ITU-T, "Functional architecture for Desktop as a Service". Recommendation Y.3504, June 2016.

13. ITU-T, " Cloud computing – Functional architecture for Network as a Service". Recommendation Y.3515, July 2017.

14. ITU-T, " Cloud computing – Functional architecture for intercloud computing". Recommendation Y.3516, September 2017.

15. Nazarov, A., Nazarov, M., Pantiuhin, D, Pokrova, S., & Sychev, A 2015, ′Automation of monitoring processes in web-based neuro-fuzzy formalism′, T-comm – Telecommunications and Transport, vol. 9, no. 8, pp. 26-33.

16. A.N. Nazarov, Alireza Nik Aein Koupaei, Anshita Dhoot, Asyraf Azlan & Seyed Milad Ranaei Siadat 2020, ′Mathematical Modelling of Infrastructure as a Service′, paper presented in the annual Collection of scientific works of International Scientific Conference "2020 SYSTEMS OF SIGNALS GENERATINGAND PROCESSING IN THE FIELD OF ON BOARD COMMUNICATIONS", (IEEE Conference #48371), Moscow Technical University of Communication and Informatics (MTUCI), Institute of Electrical and Electronics Engineers (IEEE), Media Publisher Ltd, 2020, 7 p. – in press.

17. Nazarov, A 2019, ′Model of parallel processing of tasks in the cloud cluster Hadoop′, paper presented in the Collection of proceedings of XIII International Industry Conference "Information Society Technologies", Russia, Moscow Technical University of Communications and Informatics, The Publishing House Media publisher, March 20-21, 2019. In 2 volumes, Vol. 2, pp.69-71.

18. Grigoriev, V & Nazarov, A 2019, ′Methodological aspects of parallel problem solving in the cloud cluster of cyber-attacks monitoring′, paper presented in the Collection of proceedings of XVIII scientific and practical conference "Information technologies in public administration. Digital transformation into human capital", Russia, Moscow, Federal state unitary enterprise "Research Institute "Voskhod", April 25, pp. 28-32.

19. Nazarov, A 2019, ′Processing streams in a monitoring cluster′, Russian Technological Journal, Vol. 7, № 6, pp. 54-65. https://doi.org/10.32362/2500-316X-2019-7-6-56-67

20. A.N. Nazarov, Pramod Narayan Tripathi, M Asif Hasan & Duong Viet Tung, 2020, ′ Virtual connections for IaaS service tenants′, paper presented in the annual Collection of scientific works of International Scientific Conference «2020 Wave electronics and its application in information and telecommunication systems (WECONF – 2020, IEEE Conference #48837)». Saint Petersburg State University of Aerospace Instrumentation. June 01-05, 2020, 5 p., - in press.

21. Nazarov, A & Sychev, K 2011, Models and methods for calculating the indicators of quality of functioning of the equipment units and structural parameters of the network the next generation networks, 2th edn, LLC Policom, Russia, Krasnoyarsk, 491 p.