Обоснование требований информационной безопасности туманных вычислений

Т. М. Татарникова
Санкт-Петербургский государственный
электротехнический университет
«ЛЭТИ» им. В.И. Ульянова (Ленина)
tm-tatarn@yandex.rul

В. В. Грызунов[1], А. Ю. Куманяева[2]
Российский гидрометеорологический университет
[1]viv1313r@mail.ru, [2]a.k0204@yandex.ru

***Аннотация*. Современные информационные системы имеют тенденцию к использованию туманных вычислений. Безопасность устройств, использующих туманные вычисления, зависит не только от программно-аппаратных решений, но и действий владельцев устройств тумана, от юрисдикции мест, где расположены устройства. В статье обосновываются требования информационной безопасности, позволяющие снизить риски. Исследование проводилось методом морфологического анализа с последующим введением лингвистической переменной. В результате предложены 4 категории устройств тумана: годное без ограничений, годное с незначительными ограничениями, годное с ограничениями, негодное. Выдвинуты рекомендации по организации использованию устройств тумана.**

Ключевые слова: информационная безопасность; туманныее вычисления; информационная система; категорирование объектов

I. Введение

Современные информационные системы (ИС) в поиске новых ресурсов и снижении их стоимости пришли к технологиям туманных вычислений [1]. Туманные вычисления обеспечивают недостающее звено в континууме «облако-вещь». Особенность туманных вычислений состоит в том, что вычислительный процесс перемещается ближе к потребителю результатов процесса, либо к источнику исходных данных. Устройства, применяемые для этого, называются узлами тумана. Главная задача, стоящая перед ними, – принять и выполнить задачу пользователя и/или передать её другому устройству.

При этом узлы тумана в общем виде могут быть неавторизованными устройствами, которыми владеют юридические или физические лица. Некоторые устройства самостоятельно перемещаются в пространстве и изменяют конфигурацию ИС, т. е. являются активными и слабоуправляемыми [2]. Таким образом, получается, что узел тумана находится в неконтролируемой зоне [3]. Неконтролируемость устройства приводит к возможному нарушению целостности, конфиденциальности и доступности обрабатываемых данных.

Исследование выполнено при финансовой поддержке Минобрнауки России (грант ИБ) Проект №08/2020

Вопросы обеспечения информационной безопасности (ИБ) узлов тумана решались большим количеством авторов. В работе [4] все нарушители делятся на внутренних (авторизованных) и внешних (неавторизованных), предлагается промоделировать работу и вынести решение, атакуется ИС или нет, на основе марковских цепей, систем обнаружения атак (IDS) и honeypot. Авторы в работах [5, 6] предлагают двустороннюю аутентификацию и применение инфраструктуры открытых ключей, чтобы избежать атаки «man-in-the-middle» и других возможных атак.

Узел тумана может включиться и выключиться в любой момент времени, что серьёзно влияет на результаты всего вычислительного процесса. Эта проблема решается на уровне программно-аппаратного обеспечения в работе [7] путём запрета самовольного выхода из тумана вычислительного устройства. Авторы в [8] ввели уровни надёжности устройств, рассчитываемых в процессе эксплуатации. В работе [9] предлагается строить защиту вычислительного процесса на основе активных данных.

Однако ИС является иерархической системой [10], в которой персонал является метасистемой для программного и аппаратного обеспечения. И уровни программного и аппаратного обеспечения функционируют так, как будет угодно персоналу. Это означает, что техническими методами, предлагаемыми другими авторами, сложно решить проблему узлов тумана, вызванную человеческим фактором. И все предложенные предыдущими авторами методы и способы нивелируются владельцем узла тумана путём загрузки троянов, клавиатурных шпионов, руткитов и т. п.

Цель исследования – выдвинуть требования к устройствам узлов тумана и их владельцам, позволяющие снизить риски информационной безопасности.

Исследование проводилось методом морфологического анализа с последующим введением лингвистической переменной. В ходе исследования учитывались основные влияющие на организацию вычислительного процесса свойства владельцев устройств тумана, особенности обрабатываемых данных, характеристики устройств тумана. Сложность исследования заключалась в том, что с одной стороны, показатели должны претендовать на полноту, с другой, – их не должно быть очень много, так как большое количество показателей делает невозможным их практическое применение.

II. Параметры морфологического анализа и их значения

Согласно правовому статусу, владельцы устройств тумана являются физическими и юридическими лицами

A. Свойства физических лиц

- здравомыслие – способность верно судить и отличать истинное от ложного (Декарт). Это важно, потому что человек должен понимать и принимать риски и ответственность, возникающие при сдаче своего устройства в аренду;
- зависимость жизни и здоровья от работоспособности устройства [11];
- нарушение законодательства в сфере информационных технологий и не только. Непосредственное взаимодействие с вычислительными системами такого масштаба могут одурманить разум, и все что используется во благо, может быстро поменять полярность;
- наличие статуса иностранного агента.

B. Свойства юридических лиц

- наличие у ИС аттестата соответствия. ИС, принадлежащая юридическому лицу, имеет свой уровень защищенности, который подтверждается аттестатом контролирующего органа;
- наличие статуса иностранного агента.

C. Характеристики устройства тумана

В работе [12] обосновывается, что ИС безразлично смысловое наполнение решаемых задач. ИС важно знать сколько, на какой срок и какой именно производительности нужно выделить задаче. Любая задача описывается в виде производительностей четырех типов (вычислителей, каналов связи, устройств ввода/вывода, памяти). Таким образом, понимание устройства тумана, предлагаемое в [1], расширяется до устройств, предоставляющих каналы связи, память и устройства ввода/вывода.

Наличие требуемой производительности устройства обусловлено такими техническими характеристиками как:

- использование лицензионного программного обеспечения (ПО), – распространение вредоносных кодов и использование уязвимостей в ПО больше характерно для нелицензионного ПО;
- располагаемый устройством запас энергии, – от этого показателя зависит не только возможность туманных вычислений, но и жизнедеятельность самого владельца устройства [13];
- использование сертифицированного ПО, – некоторые задачи требуют именно сертифицированного ПО;
- наличие на устройстве тумана средств разработки и отладки ПО, – определяет способности владельца устройства вмешиваться в процесс решения задачи пользователя туманных вычислений;
- использование на устройстве стандартного набора средств защиты информации: антивирус, межсетевой экран;
- тип и объём производительности, которую позволяет арендовать владелец устройства;
- лимитное подключение к системе передачи данных. Поскольку мы рассматриваем туманные вычисления, предполагается, что такой системой выступает сеть Интернет – важный аспект в жизни каждого пользователя сети. Среднестатистический человек находиться в интернете больше половины своего свободного времени. Многие давно перешли на режим безлимитного сетевого трафика, но некоторых объем передаваемых данных все же волнует.

D. Свойства данных, обрабатываемых в тумане

Законодательно выделяется открытая, запрещённая информация и информация ограниченного доступа (рисунок). Исходя из этого, необходимо предъявлять разные требования к устройствам тумана.

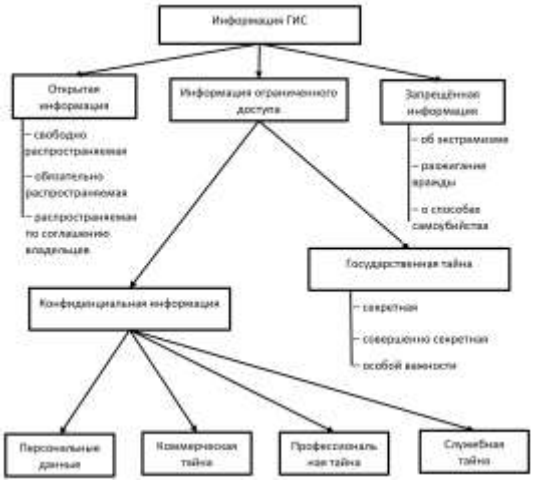

Рис. 1. Классификация информации ГИС по режиму доступа

III. Категорирование устройств тумана

Исходя из предложенных показателей оценивания устройств тумана, предлагается следующее категорирование:

A. Категория А – устройство годно для использования в туманных вычислениях без ограничений

- владелец устройства – юридическое лицо, которое имеет аттестат соответствия, позволяющий обрабатывать данные, планируемые на устройство тумана;
- владелец устройства не является иностранным агентом;

- заключен соответствующий договор на эксплуатацию устройства;
- на устройстве используется лицензионное ПО;
- на устройстве используется сертифицированное ПО;
- на устройстве отсутствуют средства разработки и отладки ПО;
- заряд батареи более 90 % для мобильного устройства;
- владелец устройства гарантирует, что производительность не упадёт ниже минимального гарантированного значения в рамках оговорённого времени;
- безлимитный доступ в Интернет.

B. категория Б – устройство годно для использования в туманных вычислениях с незначительными ограничениями

- владелец устройства – юридическое лицо или физическое лицо, не судимое ранее, в отношении которого не ведётся уголовное преследование, не состоящее на учете в полиции или неврологических и наркологических диспансерах, здоровье не зависит от использования устройства;
- заключен соответствующий договор на эксплуатацию устройства, возможно в форме оферты;
- владелец устройства не является иностранным агентом;
- на устройстве используется лицензионное ПО;
- на устройстве используется сертифицированное ПО;
- на устройстве используется стандартный набор средств защиты информации: антивирус, межсетевой экран;
- на устройстве отсутствуют средства разработки и отладки ПО;
- заряд батареи более 70 % для мобильного устройства;
- владелец устройства гарантирует, что производительность не упадёт ниже минимального гарантированного значения;
- безлимитный доступ в Интернет.

C. категория В – устройство годно с ограничениями для использования в туманных вычислениях

- владелец устройства – юридическое лицо или физическое лицо, здоровье не зависит от использования устройства;
- заключен соответствующий договор на эксплуатацию устройства, возможно в форме оферты;
- на устройстве используется лицензионное ПО;
- заряд батареи более 30 % для мобильного устройства;
- лимитированный доступ в Интернет.

D. категория Г – устройство не годно для применения в туманных вычислениях

В остальных случаях.

IV. Рекомендации по организации использования устройств тумана

Риски и ответственность, возникающие при использовании устройства тумана, регламентируются подписанием соглашения о присоединении к туману.

Владельцы устройств тумана сами должны иметь право выбирать категорию информации, которые их устройства могут обрабатывать, а также объём ресурса, который сдаётся в аренду, и временные промежутки, когда используется устройство. Пользователи туманных вычислений (Fog-As-a-Service) также должны выбирать категорию устройств, на которые могут назначаться их задачи.

Для обеспечения целостности и конфиденциальности обрабатываемых данных на устройстве тумана целесообразно использовать средства виртуализации.

V. Заключение

Практически любые задачи могут быть реализованы с помощью туманных вычислений при соблюдении соответствующих требований. Все устройства тумана сведены в 4 категории: А – устройство годно без ограничений, Б – устройство годно с незначительными ограничениями, В – устройство годно с ограничениями, Г – устройство не годно для применения в качестве узла тумана.

Участие в туманных вычислениях – сугубо добровольный процесс, однако, особо следует изучить возможность принудительного использования устройств тумана, например, в режиме чрезвычайной ситуации или военной опасности.

Необходимо разработать методику категорирования устройств тумана.

Авторы понимают, что в статье выдвинуты гипотезы, которые предстоит проверить на практике и обсудить в официально созданных рабочих группах специалистов из разных сфер человеческой деятельности.

Список литературы

[1] IEEE Standard Association et al. IEEE 1934-2018-IEEE standard for adoption of open-fog reference architecture for fog computing, 2018.

[2] Грызунов В.В. Модель информационно-вычислительной системы, деградирующей в условиях информационно-технических

воздействий // Военно-космическая академия им. А.Ф.Можайского: труды. 2015. Вып. 646. Март. С.93-102.

[3] Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014) [Электронный ресурс]. URL: https://sudact.ru/law/metodicheskii-dokument-mery-zashchity-informatsii-v-gosudarstvennykh/metodicheskii-dokument/3/3.12/zts.2-organizatsiia-kontroliruemoi-zony-v/ (дата обращения: 14.03.2021)

[4] Sohal A.S. et al. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments // Computers & Security. 2018. Т. 74. P. 340-354.

[5] Stojmenovic I. et al. An overview of fog computing and its security issues // Concurrency and Computation: Practice and Experience. 2016. Т. 28. №. 10. P. 2991-3005.

[6] Кругликов С.В., Дмитриев В.А., Степанян А.Б., Максимович Е.П Информационная безопасность информационных систем с элементами централизации и децентрализации // Вопросы кибербезопасности. 2020. № 1 (35). С. 2-7.

[7] Jia B. Double-matching resource allocation strategy in fog computing networks based on cost efficiency / B. Jia et al. // Journal of Communications and Networks, 2018. Iss. 20, № 3. P. 237–246. DOI 10.1109/JCN.2018.000036.

[8] Sun Y. Multi-objective optimization of resource scheduling in fog computing using an improved NSGA-II / Y. Sun, F. Lin, H. Xu // Wireless Personal Communications, 2018. Vol. 102. № 2. P. 1369–1385. DOI 10.1007/s11277-017-5200-5.

[9] Маркин Д.О., Макеев С.М., Вихарев А.Н. Комплекс алгоритмов защищенных туманных вычислений на основе технологии активных данных. Известия ТулГУ. Технические науки. 2019. Вып. 3, с.263-269.

[10] Грызунов В.В. Аналитическая модель целостной информационной системы // Доклады ТУСУР. 2009. № 1(19), ч.1. С.226-230.

[11] Роль Интернета в социализации людей с ограниченными возможностями здоровья [Электронный ресурс]. URL: https://medconfer.com/node/11264 (дата обращения: 14.03.2021).

[12] Грызунов В.В. Метод динамического формирования пулов в информационно-вычислительных системах военного назначения // Информационно-управляющие системы. 2015. № 1. С.13-20. doi:10.15217/issn1684-8853.2015.1.13.

[13] Detection System for Threats of the Presence of Hazardous Substance in the Environment / B.Y. Sovetov, T.M. Tatarnikova and V.V. Cehanovsky // 2019 XXII International Conference on Soft Computing and Measurements (SCM)) / St. Petersburg, Russia, 2019. P. 121-124, DOI: 10.1109/SCM.2019.8903771

.