Анализ методов обхода ориентированного графа

Пестов Игорь Евгеньевич
старший преподаватель Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ip@sut.ru

Федоров Павел Олегович
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, pavel_lenin@mail.ru

Федорова Екатерина Сергеевна
студент Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, г. Санкт-Петербург, Россия, ek.chukina@yandex.ru

АННОТАЦИЯ

Введение: В данной работе рассматривается проблема информационной безопасности инстансов облачной инфраструктуры**. Цель исследования**: В приведенной работе было необходимо провести анализ методов обхода ориентированного графа. **Результаты**: В данной статье был рассмотрен структурный подход представления информационной системы, основанный на описании компонентов информационной системы, а также их метрик, и информационных потоков между ними средствами теории графов. Был проведен анализ алгоритмов обхода ориентированного графа и их временной сложности. Было описано программно-техническое средство, созданное нами, значительно упрощающее данный анализ. С помощь данного средства было проверено утверждение, что из-за разницы в работе алгоритмов, edge_dfs требуется больше времени для выполнения задачи, чем dfs_edges. В качестве экспериментальной проверки выдвинутой гипотезы и для оценки эффективности работы программно-технического средства, был произведен теоретический и экспериментальный расчет временной сложности алгоритмов для графов с различным количеством узлов и вершин. **Практическая значимость:** данный анализ позволяет повысить эффективность построения модели безопасности облачной инфраструктуры. **Обсуждение:** в качестве дальнейшей работы, можно рассмотреть перспективу расширения количества методов обхода обрабатываемых нашим программно-техническим средством.

КЛЮЧЕВЫЕ СЛОВА: облачная инфраструктура; информационная безопасность; метрика; инстанс; теория графов; алгоритм обхода.

Введение

Современный этап развития общества характеризуется возрастающей ролью информации, рассматривающийся как один из основных ресурсов информационного общества. В связи с высокими темпами развития информационных технологий и технических средств проблема защиты информации в информационных системах становиться все более актуальной. Для обеспечения безопасности информационных систем необходимо разработать эффективную систему защиты информации, представляющую собой комплекс организационно технических мер и программно-технических средств, направленных на противодействие источникам угроз безопасности информации.

Для построения адекватной системы защиты информации нужно разработать модель угроз безопасности. Важным этапом разработки модели является описание информационной системы, так как правильность и полнота общей характеристики, включающей описание структурно функциональных данных, алгоритмов работы и технологий обработки информации, дает возможность идентифицировать все актуальные угрозы безопасности, и, как следствие, грамотно разработать систему защиты информации.

В данной статье рассмотрен структурный подход представления информационной системы, основанный на описании компонентов информационной системы, а также их метрик, и информационных потоков между ними средствами теории графов. Теория графов - один из главных инструментов математики, используемый для представления множеств и связей между ними. Граф представляет из себя топологическую модель, состоящая из определенного множества вершин и множества соединяющих их рёбер. Смысловое значение при построении графа имеет только сам факт, какая вершина с какой имеет соединения. Иными словами, можно описать граф как структуру данных, составляющую сети с парными связями внутри.

Многие задачи решаются с использованием богатейшей библиотеки алгоритмов теории графов. Для этого достаточно лишь принять объекты за вершины, а связь между ними - за рёбра, после чего все многообразие алгоритмов теории помогает в решении поставленной задачи. С помощью графов можно представить абсолютно любую структуру или систему, от транспортной сети до сети передачи данных и от взаимодействия белков в ядре клетки до связей между людьми в Интернете. В данной статье приведен анализ алгоритмов обхода ориентированного графа, и описано программно-техническое средство, созданное нами, упрощающее этот анализ.

Обход графа в ширину и глубину

Обходом графа принято называть процесс перехода от одной вершины к другой для поиска свойств связей этих вершин. Под связями в данном случае понимаются направления, пути или ребра графа. Вершины графа также называют узлами. Двумя основными алгоритмами обхода графа являются поиск в глубину (Depth-First Search, DFS) и поиск в ширину (Breadth-First Search, BFS).

DFS (англ. depth-first search) – это рекурсивный алгоритм для обхода графа, следующий концепции «погружайся глубже, головой вперед» («go deep, head first»). Суть данного алгоритма в том, что движение по графу происходит от начальной точки по определенному пути до тех пор, пока не будет достигнут конец графа или точка назначения (искомая вершина). Пример ориентированного графа представлен на рисунке 1.

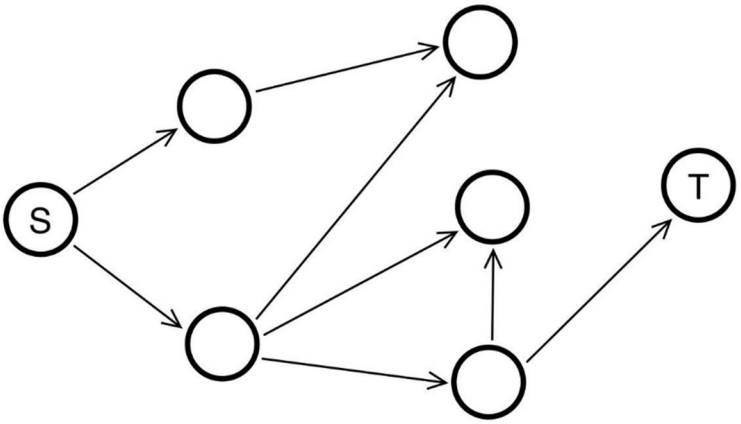

Рис.1. Ориентированный граф

Движение при данном алгоритме начинается из точки «S» с целью попадания в точку «T». Используя DFS, движение происходит в одном из возможных направлений до тех пор, пока точка «T» не будет обнаружена. В случае если по одному из направлений точки «T» не было обнаружено, алгоритм возвращает процесс обхода к исходной точке «S» и движение происходит по другому пути. Наглядно этот процесс представлен на рисунке 2.

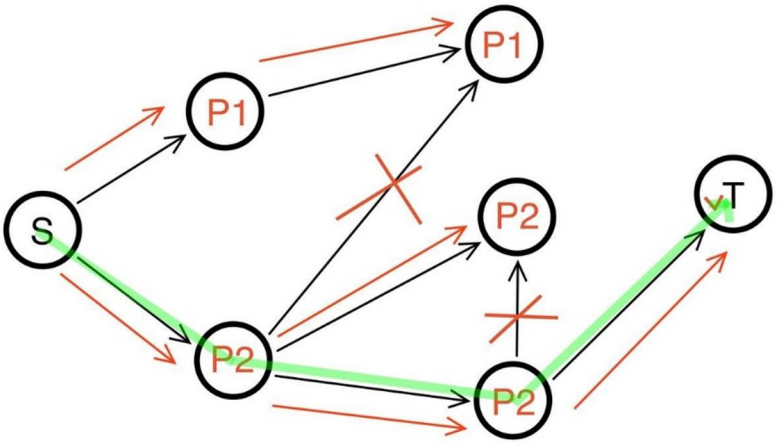

Рис.2. Путь обхода ориентированного графа

Анализируя данный алгоритм, видим, что при обходе каждого «соседа» каждого узла, пропуская тех, которых посещали ранее, имеем время выполнения алгоритма, вычисляемое по формуле 1 и равное T.

$$T = O(V + E) \tag{1}$$

где:

V- общее количество вершин,

E – общее количество граней (ребер).

Может показаться, что корректней использовать в формуле произведение вершин и граней, но это бы означало, что применительно к каждой вершине, мы должны исследовать все грани графа безотносительно принадлежности этих граней к конкретной вершине. В

нашем же случае мы оцениваем лишь примыкающие к каждой вершине грани. Каждая вершина имеет определенное количество граней и, в худшем случае, мы обойдем все вершины (O(V)) и исследуем все грани (O(E)), а так как мы имеем V вершин и E граней, то получаем E+V. Пространственная сложность алгоритма составляет O(V).

Алгоритм обхода BFS следует концепции «расширяйся, поднимаясь на высоту птичьего полета» («go wide, bird's eye-view»). Движение при данном алгоритме начинается из точки «S» с целью попадания в точку «T», но взамен концепции движения по определенному пути до конца, BFS предполагает движение вперед по одному соседнему узлу за раз, посещая ближайших к начальной точке «S» соседей. Затем движение происходит к соседним узлам этих соседних узлов до момента обнаружения конечной точки «T». Наглядно этот процесс представлен на рисунке 3.

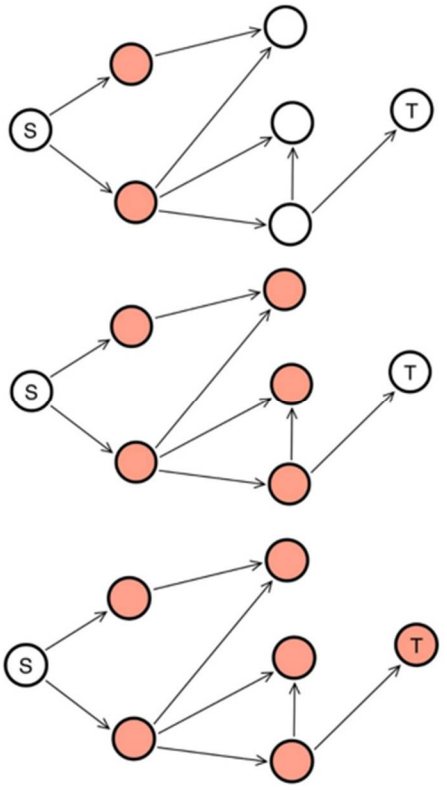

Рис.3. Путь обхода ориентированного графа в ширину

При анализе работы данного алгоритма может показаться что он работает медленней чем DFS, однако если внимательно присмотреться к визуализациям, можно увидеть, что время выполнения у них одинаково. Очередь предполагает обработку каждой вершины перед достижением пункта назначения. Это означает, что, в худшем случае, BFS исследует все вершины и грани. Таким образом, время выполнения BFS также вычисляется по формуле 1, а поскольку мы используем очередь, вмещающую все вершины, его пространственная сложность также составляет O(V).

Исследование разновидностей алгоритма обхода ориентированного графа в глубину.

В данной статье были рассмотрены разновидности алгоритма обхода ориентированного графа в глубину и было проведено исследование этих разновидностей на предмет скорости работы. В целях исследования на языке программирования Pyton была написана программа выводящая время работы алгоритма. Для анализа использовались две разновидности алгоритма обхода в глубину dfs_edges и edge_dfs которые немного отличаются друг от друга принципом работы.

Dfs_edges двигается в направлении конца графа до тех пор, пока не достигнет его. Затем он просто останавливается и завершает свою работу. Реализация этой функции адаптирована из функции поиска глубины Дэвида Эппштейна с изменениями, допускающими ограничения глубины. Если источник не указан, то источник выбирается произвольно и многократно до тех пор, пока не будут найдены все компоненты в графе.

Edge_dfs же в свою очередь работает немного иначе. Так же двигаясь в определенном направлении для достижения конечной точки, он должен обойти все возможные ребра, так как целью этой функции является посещение краев.

Написанная нами программа для определения времени работы алгоритмов обхода графа в глубину на начальном своем этапе строит ориентированный граф, используя метрики инстансов тестовой облачной инфраструктурами, принятой нами за информационную систему к которой строиться модель обнаружения угроз безопасности, как вершины графа.

На дальнейшем этапе работы программы происходит анализ времени работы алгоритмов обхода графа в глубину.

```
print("Первый алгоритм обхода графа в глубину:")
tic2 = time.perf_counter()
print(list(networkx.dfs_edges(g, 'SXS')))
toc2 = time.perf_counter()
print(f"Вычисление заняло {toc2 - tic2:0.4f} секунд \n")
```

Рис.5. Алгоритм обхода в глубину dfs_edges

```
print("Второй алгоритм обхода графа в глубину:")
tic3 = time.perf_counter()
print(list(networkx.edge_dfs(g, 'SXS')))
toc3 = time.perf_counter()
print(f"Вычисление заняло {toc3 - tic3:0.4f} секунд \n")
```

Рис.6. Алгоритм обхода в глубину edge_dfs

Из-за разницы в работе алгоритмов, edge_dfs требуется больше времени для выполнения задачи, чем dfs_edges. Об этом же утверждении свидетельствует и вывод программы, представленный на рисунке 7.

```
Первый алгоритм обхода графа в глубину:
[('SXS', 'CPU'), ('CPU', 'RAM'), ('RAM', 'ST'), ('ST', 'NET'), ('NET', 'N1'),
Вычисление заняло 0.0001 секунд

Второй алгоритм обхода графа в глубину:
[('SXS', 'CPU'), ('CPU', 'RAM'), ('RAM', 'ST'), ('ST', 'NET'), ('NET', 'N1'),
Вычисление заняло 0.0003 секунд
```

Рис.7. Вывод программы

Оценка эффективности

Для оценки эффективности написанной нами программы был проведен ряд экспериментов с увеличением количества вершин и ребер ориентированного графа. Для начала был взят граф 1 с девятнадцатью вершинами и восемнадцатью узлами. Граф представлен на рисунке 8.

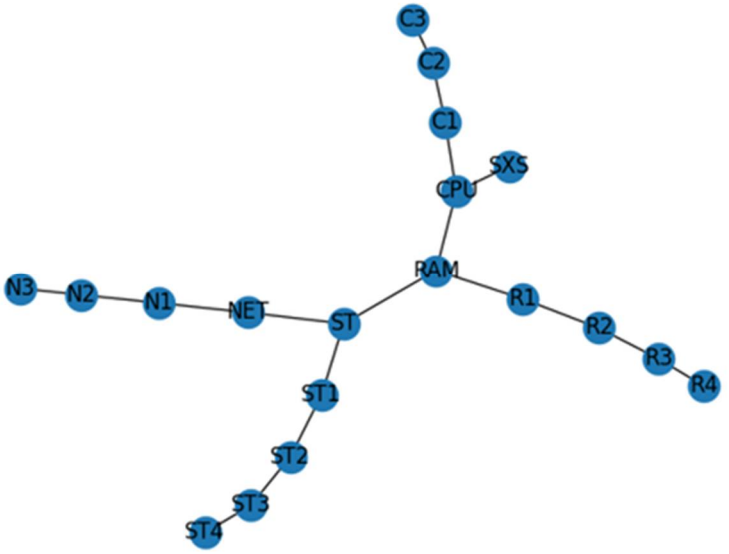

Рис.8. Ориентированный граф 1 с метриками инстансов облачной инфраструктуры

Затем по формуле 1 произведены расчеты теоретического времени работы алгоритмов. При подстановке необходимых переменных в код программы получены экспериментальные значения времени работы алгоритма. Результаты эксперимента представлены в таблице 1.

Таблица 1

Зависимость времени вычисления от количества вершин и узлов графа 1

Алгоритм	Вершин	Узлов	Время теор.(T1), с	Время эксп. (T2), с
dfs_edges	19	18	0,0002	0,0001
edge_dfs			0,0004	0,0003

Для оценки эффективности работы программы были произведены расчеты разницы между теоретическим значением времени выполнения алгоритма и экспериментальным. Расчеты для алгоритма dfs_edges первого графа производились по формуле 2.

$$\Delta T_1 = T1 - T2$$
$$\Delta T_1 = 0,0001 \tag{2}$$

Расчеты для алгоритма edge_dfs первого графа производились по формуле 3.

$$\Delta T_2 = T1 - T2$$
$$\Delta T_2 = 0,0001 \tag{3}$$

На втором этапе был взят граф 2 с тридцатью восьмью вершинами и тридцатью семью узлами. Граф представлен на рисунке 9.

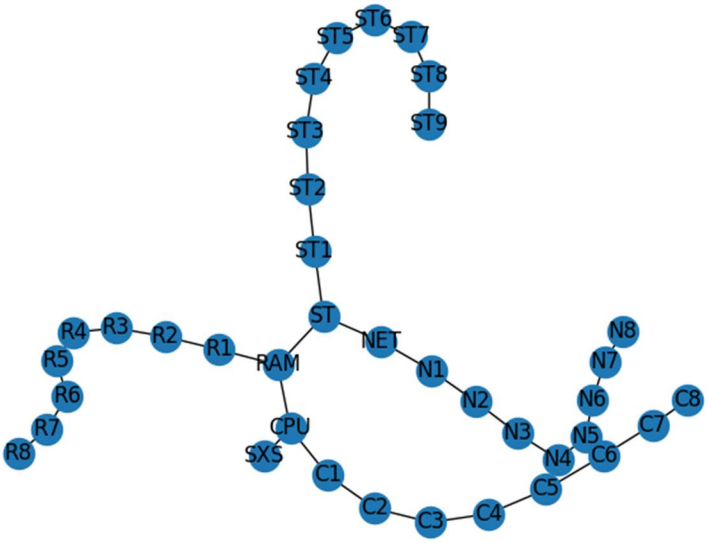

Рис.9. «Ориентированный граф 2 с метриками инстансов облачной инфраструктуры»

Расчеты времени выполнения алгоритма производились по аналогии с первым этапом эксперимента. Результаты представлены в таблице 2.

Таблица 2

Зависимость времени вычисления от количества вершин и узлов графа 2

Алгоритм	Вершин	Узлов	Время теор.(T3), с	Время эксп. (T4), с
dfs_edges	38	37	0,0002	0,0001
edge_dfs			0,0003	0,0002

Расчеты для алгоритма dfs_edges второго графа производились по формуле 4.

$$\Delta T_3 = T3 - T4$$
$$\Delta T_3 = 0,0001 \quad (4)$$

Расчеты для алгоритма edge_dfs второго графа производились по формуле 5.

$$\Delta T_4 = T3 - T4$$
$$\Delta T_4 = 0,0001 \quad (5)$$

На третьем этапе был взят граф 3 с девятнадцатью вершинами и двадцатью четырьмя узлами. Граф представлен на рисунке 10.

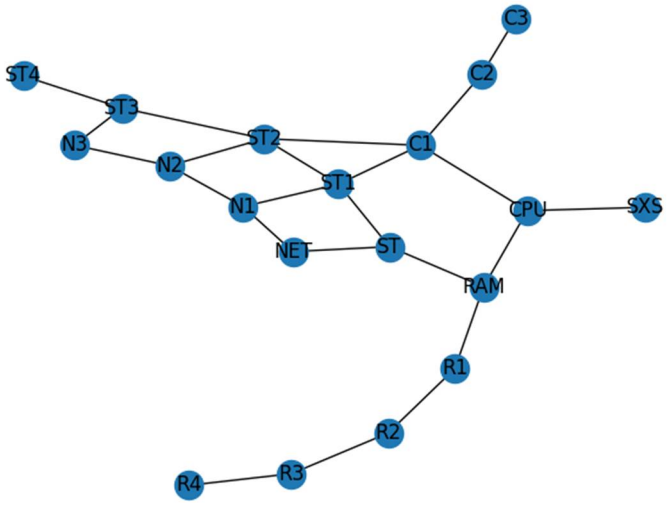

Рис.10. Ориентированный граф 3 с метриками инстансов облачной инфраструктуры

Расчеты времени выполнения алгоритма производились по аналогии с первым и вторым этапом эксперимента. Результаты представлены в таблице 3.

Таблица 3

Зависимость времени вычисления от количества вершин и узлов графа 3

Алгоритм	Вершин	Узлов	Время теор.(T5), с	Время эксп. (T6), с
dfs_edges	19	24	0,0003	0,0002
edge_dfs			0,0004	0,0003

Расчеты для алгоритма dfs_edges второго графа производились по формуле 6.

$$\Delta T_5 = T5 - T6$$
$$\Delta T_5 = 0,0001 \quad (6)$$

Расчеты для алгоритма edge_dfs второго графа производились по формуле 7.

$$\Delta T_6 = T5 - T6$$
$$\Delta T_6 = 0,0001 \quad (7)$$

Заключение

Исходя из полученных результатов видим, что разница между теоретическим и экспериментальным значением временной сложности алгоритмов обхода графа в глубину минимальна, что подтверждает эффективность нашей программы и делает возможным ее применение практике для анализа модели представленной в виде графа с любым количеством узлов и вершин.

Также экспериментальная проверка подтвердила утверждение о наибольшей производительности алгоритма dfs_edges. Данный алгоритм однозначно ускоряет процесс анализа информационных систем, которые могут быть представлены в виде ориентированных графов, на предмет информационной безопасности. Такой инструмент удобен и рекомендуем к использованию при построении модели угроз безопасности облачной инфраструктуры, и значительно рационализирует данный процесс. Так же он может быть использован и в построении модели безопасности других информационных систем с равнозначной эффективностью, входя в комплекс организационно технических мер и программно-технических средств, направленных на противодействие источникам угроз безопасности информации.

Литература

1. *Темченко В. И., Цветков А. Ю.* Проектирование модели информационной безопасности в операционной системе //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 740-745.

2 *Красов А.В., Штеренберг С.И., Голузина Д.Р* Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей //Электросвязь. 2019. № 11. С. 39-47.

3. *Волкогонов В. Н., Гельфанд А. М., Деревянко В. С.* Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.

4. *Гельфанд А. М., Косов Н. А., Красов А. В., Орлов Г. А.*, Защита для распределенных отказов в обслуживании в облачных вычислениях //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 329-334.

5. *Гельфанд А.М., Косов Н.А., Красов А.В., Орлов Г.А.* Защита для распределенных отказов в обслуживании в облачных вычислениях // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). сборник научных статей VIII Международной научно-технической и научно-методической конференции : в 4 т.. 2019. С. 329-334.

6. *Андрианов В.И., Виткова Л.А., Сахаров Д.В.* Исследование алгоритма защиты общедоступных персональных данных в информационных системах В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. сборник научных статей V международной научно-технической и научно-методической конференции. 2016. С. 227-231.

7. *Красов А.В., Штеренберг С.И., Москальчук А.И.* Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. № 3 (88). С. 38-46.

8. *Штеренберг С.И., Москальчук А.И., Красов А.В*. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения //Информационные технологии и телекоммуникации. 2021. Т. 9. № 1. С. 47-58.

9. *Красов А.В., Левин М.В., Фостач Е.С.* Проблемы обеспечения безопасности облачных вычислений // В книге: Информационная безопасность регионов России (ИБРР-2017). Материалы конференции. 2017. С. 520-522

10. *Миняев А.А., Красов А.В*. Методика оценки эффективности системы защиты информации территориально-распределенных информационных систем // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 3. С. 26-32.

11. *Красов А.В., Сахаров Д.В., Тасюк А.А*. Проектирование системы обнаружения вторжений для информационной сети с использованием больших данных // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 1. С. 70-76.

12. *Красов А.В., Штеренберг С.И., Голузина Д.Р*. Методика визуализации больших данных в системах защиты информации для формирования отчетов уязвимостей // Электросвязь. 2019. № 11. С. 39-47.

13. *Виткова Л.А., Иванов А.И., Сергеева И.Ю.* Исследование и разработка методик оценки рисков облачных ресурсов // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 152-155

14. *Виткова Л.А., Глущенко А.А., Сахаров Д.В., Чмутов М.В*. Выбор оптимального метода оценки эффективности перехода к облачной архитектуре. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 168-171.

15. *Виткова Л.А., Иванов А.И.* Обзор актуальных угроз и методов защиты в сфере облачных вычислений. //В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 179-182.

16. *Сахаров Д.В., Левин М.В., Фостач Е.С., Виткова Л.А*. Исследование механизмов обеспечения защищённого доступа к данным, размещенным в облачной инфраструктуре. // Наукоемкие технологии в космических исследованиях Земли. 2017. Т. 9. № 2. С. 40-46.

17. *Миняев А.А., Красов А.В., Сахаров Д.В.* Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29-33

18. *Штеренберг С.И., Москальчук А.И., Коптелова В.А., Виноградова О.М.* Разработка методов обеспечения безопасности для создания уязвимых виртуальных машин и изучение методов тестирования на проникновение // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2021. № 1. С. 32-38.

19. *Minyaev A.A., Krasov A.V., Saharov D.V.* The method and methodology of efficiency assessment of protection system of distributed information systems // В сборнике: 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2020. С. 291-295

20. *Бирих Э.В., Виткова Л.А., Левин М.В., Чмутов М.В.* Развитие стандартов и руководств в сфере облачных технологий // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). Сборник научных статей VI Международной научно-технической и научно-методической конференции. В 4-х томах. Под редакцией С.В. Бачевского. 2017. С. 92-95.

ANALYSIS OF DIRECTED GRAPH TRAVERSAL METHODS

IGOR E. PESTOV,
St-Petersburg, Russia, ip@sut.ru

PAVEL O. FEDOROV,
St-Petersburg, Russia, pavel_lenin@mail.ru

EKATERINA S. FEDOROVA,
St-Petersburg, Russia, k.chukina@yandex.ru

ABSTRACT

Introduction: This paper deals with the problem of information security of cloud infrastructure instances. **Purpose:** In the above work, it was necessary to analyze the methods of traversing of directed graphs. **Results:** In this article, a structural approach to the representation of an information system based on the description of the components of an information system, as well as their metrics, and information flows between them by means of graph theory was considered. The analysis of algorithms for traversing directed graphs and their time complexity was carried out. A software and hardware tool created by us greatly simplifying this analysis was described. With the help of this tool, the statement that due to the difference in the algorithms, edge_dfs takes more time to complete the task than dfs_edges was verified. As an experimental test of the hypothesis put forward and to evaluate the effectiveness of the software and hardware, a theoretical and experimental calculation of the time complexity of algorithms for graphs with different numbers of nodes and vertices was performed. **Practical relevance**: this analysis makes it possible to increase the efficiency of building a cloud infrastructure security model. **Discussion:** as a further work, we can consider the prospect of expanding the number of traversal methods processed by our software and hardware.

Keywords: cloud infrastructure; information security; metric; instance; graph theory; traversal algorithm.

REFERENCES

1. Temchenko V.I., Tsvetkov A.Y. Designing an information security model in the operating system // Actual problems of infotelecommunications in science and education (APINO 2019). - 2019. - S. 740-745.
2. Krasov A.V., Shterenberg S.I., Goluzina D.R. Big data visualization technique in information security systems for vulnerability reporting // Telecommunications. 2019. No. 11. S. 39-47.
3. Volkogonov V. N., Gelfand A. M., Derevyanko V. S. Relevance of automated control systems // Actual problems of infotelecommunications in science and education (APINO 2019). - 2019. - S. 262-266.
4. Gelfand A. M., Kosov N. A., Krasov A. V., Orlov G. A., Protection for distributed denial of service in cloud computing // Actual problems of infotelecommunications in science and education (APINO 2019). - 2019. - S. 329-334.
5. Gelfand A.M., Kosov N.A., Krasov A.V., Orlov G.A. Protection for distributed denial of service in cloud computing // In the collection: Actual problems of infotelecommunications in science and education (APINO 2019). Collection of scientific articles of the VIII International scientific-technical and scientific-methodological conference: in 4 volumes. 2019. P. 329-334.
6. Andrianov V.I., Vitkova L.A., Sakharov D.V. Study of the algorithm for protecting publicly available personal data in information systems In the collection: Actual problems of info-telecommunications in science and education. Collection of scientific articles of the V international scientific-technical and scientific-methodical conference. 2016. S. 227-231.
7. Krasov A.V., Shterenberg S.I., Moskalchuk A.I. Methodology for creating a virtual laboratory for testing the security of distributed information systems // Bulletin of the Bryansk State Technical University. 2020. No. 3 (88). pp. 38-46.
8. Shterenberg S.I., Moskalchuk A.I., Krasov A.V. Development of security scenarios for the creation of vulnerable virtual machines and the study of penetration testing methods //Information technologies and telecommunications. 2021. V. 9. No. 1. S. 47-58.
9. Krasov A.V., Levin M.V., Fostach E.S. Problems of ensuring the security of cloud computing // In the book: Information Security of Russian Regions (ISRR-2017). Conference materials. 2017. S. 520-522
10. Minyaev A.A., Krasov A.V. Methodology for evaluating the effectiveness of the information protection system of geographically distributed information systems // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and technical sciences. 2020. No. 3. S. 26-32.
11. Krasov A.V., Sakharov D.V., Tasyuk A.A. Designing an intrusion detection system for an information network using big data // Science-intensive technologies in space research of the Earth. 2020. V. 12. No. 1. S. 70-76.
12. Krasov A.V., Shterenberg S.I., Goluzina D.R. Big Data Visualization Technique in Information Security Systems for Vulnerability Reporting // Elektrosvyaz. 2019. No. 11. S. 39-47.
13. Vitkova L.A., Ivanov A.I., Sergeeva I.Yu. Research and development of methods for assessing the risks of cloud resources // In the collection: Actual problems of infotelecommunications in science and education (APINO 2017). Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes. Edited by S.V. Bachevsky. 2017. S. 152-155.
14. Vitkova L.A., Glushchenko A.A., Sakharov D.V., Chmutov M.V. Choosing the optimal method for evaluating the effectiveness of the transition to cloud architecture. // In the collection: Actual problems of infotelecommunications in science and education (APINO 2018). VII International scientific-technical and scientific-methodical conference. Collection of scientific articles. In 4 volumes. Edited by S.V. Bachevsky. 2018. S. 168-171.
15. Vitkova L.A., Ivanov A.I. Overview of current threats and protection methods in the field of cloud computing. //In the collection: Actual problems of infotelecommunications in science and education (APINO 2018). VII International scientific-technical and scientific-methodical conference. Collection of scientific articles. In 4 volumes. Edited by S.V. Bachevsky. 2018. S. 179-182.
16. Sakharov D.V., Levin M.V., Fostach E.S., Vitkova L.A. Study of mechanisms for providing secure access to data hosted in the cloud infrastructure. // Science-intensive technologies in space research of the Earth. 2017. V. 9. No. 2. S. 40-46.

17. Minyaev A.A., Krasov A.V., Sakharov D.V. Method for evaluating the effectiveness of the information security system of geographically distributed information systems of personal data // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and technical sciences. 2020. No. 1. S. 29-33
18. Shterenberg S.I., Moskalchuk A.I., Koptelova V.A., Vinogradova O.M. Development of security methods for creating vulnerable virtual machines and the study of penetration testing methods // Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and technical sciences. 2021. No. 1. S. 32-38.
19. Minyaev A.A., Krasov A.V., Saharov D.V. The method and methodology of efficiency assessment of protection system of distributed information systems // In the collection: 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). 2020. C. 291-295
20. Birikh E.V., Vitkova L.A., Levin M.V., Chmutov M.V. Development of standards and guidelines in the field of cloud technologies // In the collection: Actual problems of infotelecommunications in science and education (APINO 2017). Collection of scientific articles of the VI International scientific-technical and scientific-methodical conference. In 4 volumes. Edited by S.V. Bachevsky. 2017. S. 92-95.