**ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ**
**INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**УДК 004.05**
**DOI:** 10.21822/2073-6185-2022-49-2-46-55 Оригинальная статья /Original Paper

# Информационная безопасность предпринимательских сетей

**А.С. Лосев**
Институт прикладной математики Дальневосточного отделения РАН,
690041, г. Владивосток, ул. Радио, 7, Россия

**Резюме. Цель.** Целью работы является повышение информационной безопасности сетей предпринимательского вида, как наиболее подверженных внешним угрозам с целью коммерческого шпионажа. **Метод.** Исследование основано на использовании оригинального математического алгоритма, позволяющего проводить кластеризацию сетей произвольной топологии и строить матрицу частичного порядка. С одной стороны, кластеризация позволяет выявить агентов сети, имеющих одинаковый информационный доступ к сети, с другой стороны, частичный порядок отражает положение отдельно взятого кластера в иерархической структуре всей сети. **Результат.** Данный подход позволяет оценить потенциальную угрозу сети в зависимости от положения агента в сети, подвергшегося атаке. На основе данного подхода разработана методика определения степени открытости предпринимательской сети к воздействию со стороны внешних факторов для каждого агента сети. Она позволяет выделить агентов сети, требующих усиления безопасности по отношению к внешнему воздействию, так как потенциальная атака на них имеет максимально негативные последствия для всего соединения, что подчеркивает практическую значимость результата. **Вывод.** Разработанная методика практически значима и может быть использована для оценки информационной безопасности или целостности сети любой природы, представимой в виде ориентированного графа.

**Ключевые слова:** информационная безопасность, агент сети, предпринимательские сети, кластеризация, частичный порядок, ориентированный граф, степень открытости сети, методика

**Для цитирования:** А.С. Лосев. Информационная безопасность предпринимательских сетей. Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(2):46-55. DOI:10.21822/2073-6185-2022-49-2-46-55

# Information security of business networks

**A.S. Losev**
Institute for Applied Mathematics, Far Eastern Branch, Russian Academy of Sciences,
7 Radio Str., Vladivostok 69004, Russia

**Abstract. Objectives.** The aim of the work is to improve the information security of business-type networks, as the most susceptible to external threats for the purpose of commercial espionage. **Method.** The study is based on the use of an original mathematical algorithm that allows clustering networks of arbitrary topology and constructing a partial order matrix. On the one hand, clustering allows you to identify network agents that have the same information access to the network, on the other hand, partial order reflects the position of a single cluster in the hierarchical structure of the entire network. **Result.** This approach allows assessing the potential threat to the network depending on the position of the agent in the network that has been attacked. On its basis, a methodology has been developed to determine the degree of openness of an entrepreneurial network to the influence of external factors for each agent of the network. It allows you to identify network agents that require increased security in relation to external influences, since a potential attack on them has the most negative consequences for the entire connection, which emphasizes the practical significance of the result. **Conclu-**

**sion.** The developed technique is practically significant and can be used to assess the information security or integrity of a network of any nature, represented as a directed graph.

**Keywords:** information security, network agent, business networks, clustering, partial order, directed graph, degree of network openness, methodology

**For citation:** A.S. Losev. Information security of business networks. Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (2): 46-55. DOI: 10.21822 /2073-6185-2022-49-2-46-55

**Введение.** Процесс всемирной глобализации по различным сферам и направлениям деятельности человечества требует новых форм взаимодействия, позволяющих быстро и оперативно принимать управленческие решения, доводить их до исполнения и реализации. Естественным образом в современном информационном обществе практически все формы взаимодействия находятся в плоскости сетевых технологий, в том числе и вновь созываемых компаний, корпораций и т.д.

Появление такого объекта хозяйственно управления, как предпринимательская сеть, имеет достаточно большую историю в мировой экономической практике [1], но именно с появлением сетевых технологий их потенциал увеличился в разы. Начав свой путь с сетевизации различных отраслевых рынков [2] и до появления институционального анализа сетевых объединений хозяйственной природы [3; 4], понимание сетей в экономическом контексте претерпело различные трансформации. Естественным образом, что в зависимости от различных аспектов (функциональное назначение, сфера деятельности, число участников и т.д.) возникает различное понимание феномена предпринимательской сети [1; 5-9]. Данное многообразие в подходах полностью коррелирует с видами и природой рассматриваемых сетей, в частности, от случайных сетей огромных размерностей [10], до статических малой, где появляется возможность изучить каждый элемент сети и его связь [11]. Существующая теория сетей в экономических исследованиях, разделяет сети на группы, в зависимости от физического, экономического или институционального расстояния между участниками сети [3]. В частности, к первой группе относятся исследования в области штандорта промышленных предприятий [12] и развития территориально-промышленных комплексов [13], а ко второй индустриальных районов [14] и промышленных комплексов [15].

Относительно предпринимательских сетей, больший интерес представляют динамические модели, характеризующие сеть в отдельные моменты времени с заданной степенью вероятности [16]. Большинство данных исследований посвящено решению задачи управления сетевых соединений [17; 18], которая практически неразрешима, как только мы говорим об онлайн соединениях произвольного вида, так как в этом случае практически все параметры принимают вероятностный характер.

Достаточно очевидно, что в современных цифровых условиях, особенно последних лет, когда многие производства переведены в дистанционный формат, предпринимательские сети теперь ассоциируются с онлайн структурами, подобно социальным. Наравне с этим необходимо подчеркнуть, что в отличие от социальных онлайн сетей, предпринимательские сети, даже построенные посредством Интернет - связей, формируются на других принципах, а значит и организованы не так хаотично.

В содержательном смысле наиболее близким определением «предпринимательская сеть» представляется, как группа организаций-участников того или иного рынка, объединившихся для эффективного использования ресурсов и специфических преимуществ для совместной реализации предпринимательских проектов [19].

Интеграция предпринимательской сферы в сетевое образование естественным образом порождает новые принципы организации и взаимодействия:

– потребность в реализации принципа заинтересованности всех участников предпринимательской сети;

– рассмотрение интеграционной деятельности организации как новаторской;

– потребность в нового рода координации средств производства, выходящие за рамки одного предпринимательского субъекта;

– рассмотрение возможностей интегрированного поведения в предпринимательской сети по передаче части функций от собственника менеджерам-профессионалам;

– использование вхождения в предпринимательскую сеть для более эффективного регулирования взаимоотношений с внешней средой;

– использование возможностей предпринимательской сети для разделения труда, специализации, кооперации, как производственного процесса, так и управленческих процессов, происходящих в субъектах предпринимательской деятельности [19].

Как результат, в отличие от традиционных холдингов, концернов, трестов, с явно выраженными громоздкими аппаратами управления, зачастую «оторванными» от производственной составляющей, сетевое объединение позволяет оптимизировать имеющийся экономический потенциал и нарастить его за счет новых возможностей и проявления синергетических эффектов сетевой структуры, которые являются предметом самостоятельных исследований [5-7].

В свою очередь это позволяет решить ряд задач, стоящих перед каждым субъектом предпринимательства: снижение производственных затрат; повышение качества управления и эффективности сбыта продукции; снижение рисков; создание новых направлений деятельности; модернизация производственной базы развитие системы сервиса и сбыта.

Наиболее распространёнными сетевыми образованиями считаются кластерные модели, в состав которых входит широкий круг участников. В общем смысле, применительно к предпринимательским сетям, считается что кластер – это объединение субъектов предпринимательской деятельности, функционирующих в пределах четко очерченных территориальных образований [2, 3]. Данное представление продиктовано естественными ограничениями правого поля, действующего на конкретной территории (город, регион, страна), в рамках которого организуется предпринимательская деятельность. Естественным образом, такие кластерные объединения приводят к дополнительным экономическим эффектам по сравнению с рядовыми предпринимательскими сетями за счет сетевых форм организации производительного цикла.

Наравне с этим велик и риск информационного шпионажа или сетевой атаки, которая в случае кластерного образования, может привести не только к нарушению работы административно-управленческого аппарата, но и негативно отразиться на самом производстве, остановка которого зачастую намного опаснее своими последствиями. И, несмотря на различные меры безопасности, формы и методы которых постоянно совершенствуются, необходимо отметить, что в случае сетевых образований они ориентированы на типовые структуры.

В то же время, замещение имущественных связей информационными, отсутствие строгих ограничений на проявление сетевых объединений, позволяют говорить об уникальности каждой отдельной предпринимательской сети. Естественным образом, актуальность приобретают задачи из теории графов, направленные на исследование различных сетевых топологий, решение которых необходимо для определения наиболее оптимальных параметров функционирования сети в целом и образующих элементов в отдельности, в частности ориентированных на устойчивость к агрессивному воздействию со стороны внешних факторов.

**Постановка задачи.** В настоящей статье вводиться понятие «степени устойчивости» предпринимательской сети к воздействию со стороны внешних факторов и предложена методика её расчёта.

Рассматривается алгоритм поиска агентов потенциально благоприятных с точки зрения внешнего агрессивного влияния и нанесения ущерба. Основная идея состоит в анализе топологии сети с помощью ранее разработанных алгоритмов и определения процента достижимых

вершин из вершины, которая подверглась атаке. В отличие от прямых задач перебора всевозможных путей, предложенный алгоритм отличается быстродействием и позволяет выделить иерархическую структуру сети на основе действующего информационного потока, а не формального представления.

Алгоритм открыт к добавлению новых вершин без необходимости перезапуска с самого начала, обладая тем самым свойством динамичности. Полученный результат, позволяет существенно повысить информационную безопасность и устойчивость предпринимательской сети в целом к потенциальным угрозам.

Введем в рассмотрение предпринимательскую сеть через математическое представление, как ориентированный граф, узлами (вершинами) которого являются агенты, а направленными дугами (ребрами) – наличие связи между ними.

Под связью между агентами с позиции информационной безопасности сети в целом положим наличие прямого доступа, для агента, который устанавливает связь (выходит ребро) ко всей информации располагающейся у агента, принимающего связь (входит ребро).

Рассмотрим в данном сетевом образовании вопрос информационной безопасности, под которой будем понимать защищенность информации и поддерживающей инфраструктуры от преднамеренных воздействий искусственного характера, направленных на нанесение ущерба владельцам информации или поддерживающей структуре. Соответственно информационной атакой на предпринимательскую сеть со стороны внешнего воздействия будем считать любое целенаправленное нарушение информационной безопасности по отношению к любой вершине сети.

Степень устойчивости выделенной вершины (агента) обозначим через *s*, и будем определять её через степень изолированности по отношению ко всей сети, исходя из того, что чем меньше она имеет связей с другими узлами, тем меньше потенциальный ущерб всей сети в результате информационной атаки по отношению к ней. А именно, для каждой вершины *i* ориентированного графа определим степень устойчивости, следующим образом:

$$s_i = 1 - h_i,$$

где $h_i$ – доля вершин от общего числа в графе, в которые можно попасть по путям в графе из вершины *i*.

Из определения достаточно очевидно, что $s \in [0; 1]$, при этом если из выделенной вершины можно попасть в любую другую вершину графа, то $s=0$, если из нее нет путей ни в какую другую вершину графа, т.е. в нее только входят ребра, то $s=1$.

Положим, что две вершины в ориентированном графе эквивалентны, если существует цикл, содержащий эти вершины, где цикл – это замкнутый путь, состоящий из последовательности вершин, соединённых ребрами, начинающийся и заканчивающийся в одной и той же вершине. Данное бинарное отношение является отношением эквивалентности на множестве всех вершин графа, т.к. обладает свойствами рефлективности, симметричности и транзитивности.

Введем понятие сетевого кластера, отличное от выше рассмотренного и основанного на функциональном разбиении сети на подсети. А именно, кластером назовем множество вершин, относящихся к одному классу эквивалентности. Соответственно, множество кластеров – есть множество классов эквивалентности.

**Методы исследования.** Введем на множестве классов эквивалентности вершин графа бинарное отношение: $p \prec q$, если в исходном графе существует путь из любой вершины класса $p$ в любую вершину класса $q$.

Очевидно, что это бинарное отношение рефлексивно, транзитивно и антисимметрично и потому является отношением частичного порядка. Сопоставим частичному порядку "$\prec$" на множестве кластеров матрицу, в которой в клетке $(p,q)$ стоит единица, если $p \prec q$, иначе в

этой клетке стоит ноль.

В работе [20] разработан алгоритм построения кластеров и матрицы частичного порядка.

**Шаг 1.** Имеется вершина 1, она первая и единственная, поэтому образует кластер 1, который добавляется во множество кластеров $K$={1}.

**Шаг 2.** Вводится матрица $a = \| a(p,q) \|_{p,q \in K}$, характеризующая отношение частичного порядка "$\prec$":

$a(p,q) = 1,$ если $p \prec q,$ иначе $a(p,q) = 0,$ для которой верно, что $a(1,1) = 1.$

**Шаг 3**. Каждая последующая вершина $(n+1)$ из которой выходит не более $m$ ребер, попадающих в множество кластеров $P$ и в которую $(n+1)$ входит не более $m$ ребер из кластеров, содержащихся в множестве $Q,$ образует новый кластер в $I_{n+1},$ и инициирует переобозначения следующих множеств:

$$A_1 = K' \setminus A,\ A_2 = R' \setminus A,\ B = I_n \setminus (A \cup A_1 \cup A_2),$$

где

$$K' = \bigcup_{p \in P} K_p,\ R' = \bigcup_{q \in Q} R_q,\ A = K' \bigcap R',$$

$$K_p = \{k \in I_n : p \prec k\},\ p \in P,\ R_q = \{k \in I_n : k \prec q\},\ q \in Q.$$

Матрицы $a$ перерасчитывается на обновленном множестве кластеров $K$ по следующему правилу:

$$a(n+1, n+1) = 1,\ a(n+1, A_1) = E,\ a(A_2, n+1) = E,\ a(A_2, A_1) = E,$$
$$a(A_1, n+1) = O,\ a(A_1, B) = O,\ a(A_1, A_2) = O,\ a(n+1, A_2) = O,$$
$$a(n+1, B) = O, a(B, n+1) = O,\ a(B, A_2) = O.$$

где $O$ – нулевая матрица соответствующего размера.

**Обсуждение результатов.** В ходе реализации представленного алгоритма происходит разбиение исходной сети на кластеры (рис. 1), особенностью которых является наличие пути между двумя любыми вершинами, что естественным образом позволяет рассчитать степень устойчивости сети к воздействию со стороны внешних факторов.

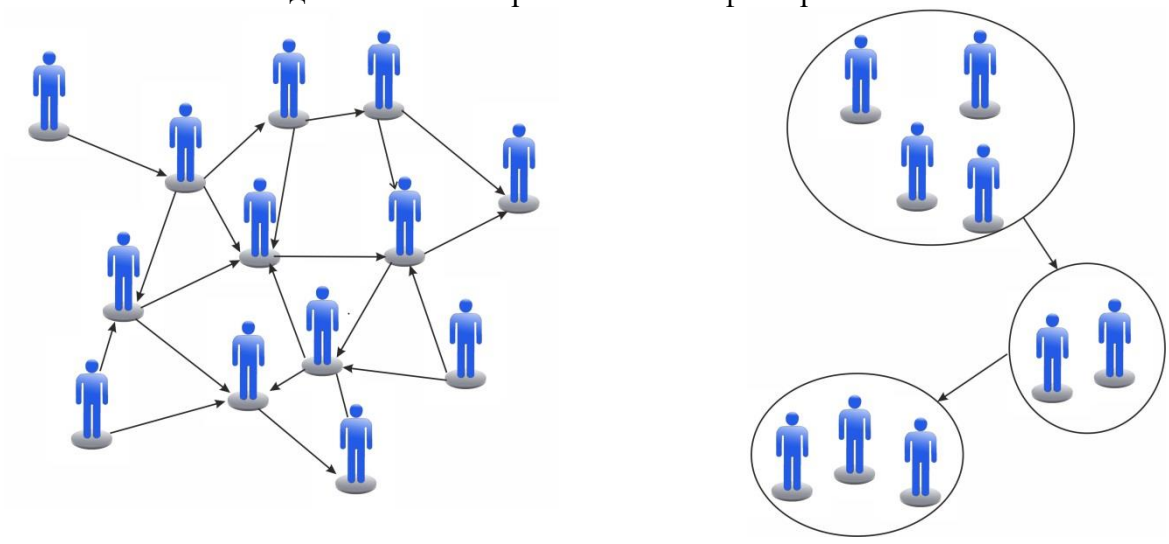

**Рис. 1. Пример графического представления сети (слева) и её кластерного разбиения (справа)**
**Fig. 1. An example of a graphical representation of the network (left) and its cluster splits (right)**

Следовательно, принадлежность агента к кластеру позволяет получить доступ к информации любого другого агента из этого кластера, либо напрямую, либо опосредованного через других агентов из этого кластера. Наравне с этим выделенный частичный порядок позволяет выделить множество кластеров, достижимых из выделенного кластера. Таким образом, доля вершин от общего числа в графе, в которые можно попасть по путям в графе из вершины *i*, определяется, следующим образом

$$h_i = \bigcup_{\{p \in K:\, p \prec i+1\}} \bigcup_{a \in K_p} a,$$

где $\{p \in K : p \prec i+1\}$ – множество, состоящее из номера кластера, содержащего вершину *i* и номеров кластеров достижимых из него; $a \in K_p$ – множество элементов из кластера $K_p$.

Заложенная в основе сетевого образования некоторая иерархия подчинения и разделения функциональных обязанностей не позволит получить доступ ко всей сети любому агенту. А именно, если проведена информационная атака на агента из нижестоящего кластера, то информация, расположенная у агентов выше в кластерной структуре, будет в безопасности. Однако если успешная информационная атака проведена в отношении агента из самого верхнего кластера, то вся информация сети подвергается угрозе (рис. 2).

Соответственно, степень устойчивости вершины в первом случае будет максимальной $s=1$, а во втором равна $s=0$.

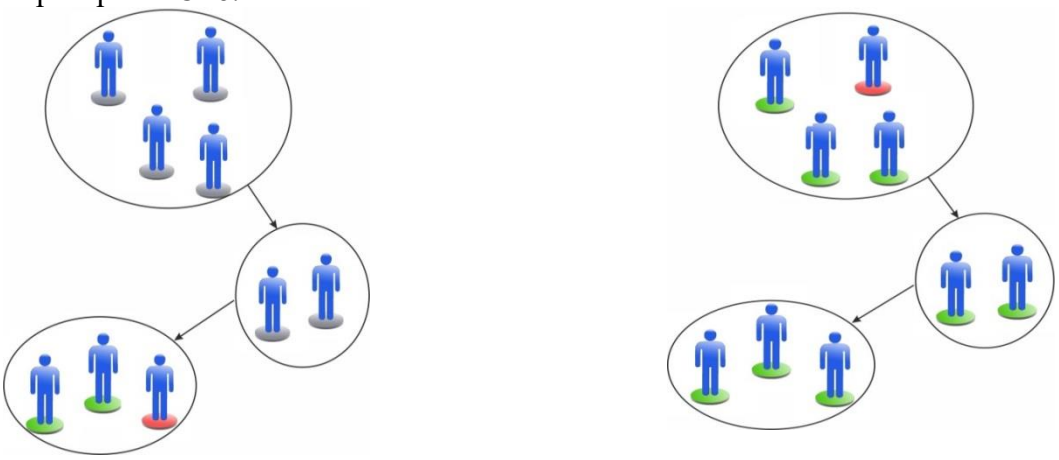

**Рис. 2. Пример нарушения информационной безопасности агентов сети (зеленым) при угрозе по отношению к выделенному агенту (красным)**

**Fig. 2. An example of information security violation of network agents (green) in case of a threat against a selected agent (red)**

Естественным образом предположить, что наиболее привлекательными со стороны внешних воздействий являются агенты с минимальной степенью устойчивости к угрозам. В основном к ним относятся сотрудники из административно-управленческого аппарата, но и уровень безопасности зачастую у них на порядок выше, чем у остальных агентов. Однако необходимо отметить, что начальное структурное разбиение, основанное на разделении обязанностей и функций, зачастую не совпадает с кластерным разбиением, основанным на наличии информационных связей. Обоснованно это тем, что функциональное разбиение носит чисто формальный характер и является статической структурой, в то время как любая информационная сеть является динамическим образованием, в которой происходит появление или нарушение связей, исходя из тех задач, которые перед ней стоят. Соответственно, организация информационной безопасности также руководствуется статистической информацией, которая обновляется периодически, но не в режиме реального времени:

– перечень требований, составляющих коммерческую тайну;

– перечень и характеристики рабочих мест, серверов и т.д.;
– описание информационных потоков и технологии обработки информации; порядок её хранения и т.п. [19]

Следовательно, вопрос информационной безопасности предпринимательской сети, большой размерности с явно выраженной иерархической структурой или малой с постоянно меняющейся топологией, намного эффективнее решать с использованием соответствующих алгоритмов, обладающих быстродействием и отражающих реальную кластеризацию, основанную на действующем информационном обороте в сети. Особенно, если учесть, что помимо прямого анализа сетевого соединения, данный алгоритм позволяет получить оценки различных характеристик сети, задействованных в её информационной безопасности, например, степень централизации сети, гетерогенность сети, ранг сети, степень структурной близости сети к сетеобразующему элементу.

Степень централизации сети характеризуется мерой группирования агентов вокруг единого центра [5]. С другой стороны, централизация – это концентрация прав принятия решений, сосредоточение властных полномочий на верхнем уровне руководства организации. Следовательно, степень централизации сети, является второстепенным показателем, участвующим в информационной безопасности. И она должна определяться не только наличием или отсутствием управляющей верхушки, но и её численностью, концентрацией и возможностью передачи решений на все уровни сети, т.е. отдаленностью самого низкого уровня сети от центра.

Предложенный алгоритм позволяет разбить сеть на кластеры, элементы которых образуют компоненты связности в ориентированном графе, порожденные исходной сетью. Помимо этого, каждый кластер, полученный в предпринимательской сети, образует совокупность агентов сети одного уровня, а отношение частичного порядка, однозначно определяет иерархию между ними. Кластер больше всех остальных по отношению частичного порядка, однозначно, определяется как управляющая верхушка, имеющая только исходящие связи и не находящиеся в подчинение, а количество выходящих связей данного кластера можно буквально считать, как степень централизации сети.

Гетерогенность сети – показатель неоднородности элементов сети. Естественным образом предположить, что функционирующая предпринимательская сеть не должна состоять только из агентов экономической сферы. Следовательно, данный показатель определяет степень агентов, связанных с предпринимательской деятельностью, но не занимающихся ею напрямую. Речь идет о вспомогательных задачах, которые необходимо решать для поддержания функционирования любой сети и не только предпринимательской. Предложенный подход в работе [5] позволяет определить процент гетерогенности сети, но мало информирует нас о расположении не предпринимательских агентов в сети, что является принципиальным с позиции информационной безопасности сети, так как именно эти агенты требуют повышенного внимания.

На основе предложенного алгоритма логично предположить, что агенты, работающие над вспомогательными задачами, в данной сети будут представляться в виде кластеров, содержащих один элемент, замыкая на себе связи, выступая связующими элементами различных отделов с внешним миром или другими сетями. Также правомерно предположить, что агенты не предпринимательской природы не должны образовывать отдельные кластеры на верхних и средних уровнях иерархии сети, в противном случае, возникает серьезное подозрение о легальности данной сети.

Следовательно, использование комбинированной оценки гетерогенности сети посредством оценки доли агентов не предпринимательской природы и их расположением в кластеризованном представлении сети, позволяет более точно охарактеризовать природу деятельности сети, предположить о законности и некой стрессоустойчивости к воздействиям на неё извне.

Ранг сети – длина общей многоступенчатой связи, в которой одни элемент сети связан с другими элементами [5]. В традиционном представлении ранг рассчитывается как среднее чис-

ло связей, входящих в маршрут связи между двумя элементами сети по кратчайшему пути, что больше соответствует средней длине между любыми двумя агентами сети. Полученный алгоритм позволяет в качестве характеристики ранга оценить длину иерархической цепочки в кластеризованной сети, тем самым определяя ранг, через количество уровней в сети, представленной через кластеры. Данное представление ранга более обоснованно с позиции практики, логики и природы сети, так вопрос об установлении количества связей, необходимых между двумя агентами одного кластера или одного уровня не актуален и в большинстве случаев решается напрямую, что нельзя сказать о порядке согласований между отделами. Следовательно, ранг будет характеризовать необходимое число уровней, которое следует согласовать или пройти для установления связи между двумя агентами сети различных уровней.

Степень структурной близости сети к сетеобразующему элементу – данный показатель может быть рассчитан в случае, если при изучении предпринимательской сети удастся установить наличие сетеобразующего элемента и однозначно его определить [5].

Определение данного показателя осложняется предварительной задачей по установлению факта присутствия сетеобразующего элемента, который не обладает четкими критериями, тем самым, носит вероятностный смысл и, в частном случае, трактуется как непосредственная связь всех элементов сети с сетеобразующим элементом. В условиях отсутствия формальных критериев поиска сетеобразующиего элемента, можно рассмотреть его в зависимости от степени централизации сети.

Из вышесказанного, степень централизации сети определяется посредством разбиения сети на кластеры и построения соответствующей иерархии.

Следовательно, если речь идет о высокоцентрализованной сети, кластеризация которой представляется в виде дерева (четкая вертикаль управления) или радиальной сети (все кластеры в непосредственном подчинении выделенного элемента), то, без сомнения, сетеобразующим элементом будет выступать кластер агентов, определяющий управление всей сети.

Соответственно, степень структурной близости сети к сетеобразующему элементу может быть определена как высокая, а численная оценка будет равна рангу сети. В случае низкоцентрализованной сети, кластеризация будет содержать неявно выраженную иерархию с большим число элементов на каждом уровне, что можно интерпретировать, как отсутствие единого сетеобразующего элемента. Соответственно, степень структурной близости сети к сетеобразующему элементу считать низкой.

В случае децентрализованной сети, в результате кластеризации будет получен один кластер, содержащий все элементы сети, следовательно, степень структурной близости сети к сетеобразующему элементу можно считать нулевой в силу отсутствия такого. Следовательно, степень структурной близости сети к сетеобразующему элементу будет отражать особенности базовой топологии сети, заложенной в основе кластерного представления сети.

**Вывод.** Использование данного алгоритма при оценке степени устойчивости сети к внешним воздействиям, имеет ряд преимуществ по отношению к известным подходам кластеризации сетевых соединений.

Во-первых, наличие кластерного порядка позволяет оценить потенциальное влияние внешних угроз, установив степень устойчивости каждого агента предпринимательской сети к воздействию со стороны внешних факторов.

Во-вторых, выделение кластеров высших порядков, в случае сетей большой размерности, позволит установить круг агентов, которые требуют более высокого уровня информационной безопасности, не по формальным признакам, принадлежащих административно-управленческому аппарату, а реально имеющих доступ к информации всей сети. В случае сетей малой размерности без явно выраженного административно-управленческого аппарата, кластеризация позволит аналогично дифференцировать уровень используемой информационной защиты, что, несомненно, в обоих случае позволит уменьшить соответствующие затраты.

В-третьих, невысокая трудоёмкость алгоритма по сравнению с традиционными подходами позволяет использовать его в реальном времени для оценки безопасности всей сети в ходе её периодического мониторинга на предмет попадания тех или иных агентов в кластер, не соответствующий их уровню допуска, в результате выполнения каких-либо оперативных поручений.

В-четвертых, в отличие от традиционных алгоритмов выделения кластеров или подсетей, предложенный алгоритм не требует каждого перезапуска в случае добавления новых вершин и формирует иерархическую структуру взаимного расположения полученных кластеров.

На основе отмеченных особенностей можно разработать соответствующую методику мониторинга потенциально привлекательных агентов сети с позиции внешнего влияния. Идея состоит в мониторинге сетевого соединения предложенным алгоритмом в режиме реального времени, направленного на:

- усиление безопасности отдельных агентов сети, меняющих свое положение в кластеризованном графе с нижнего на высший уровень;
- усиление безопасности отдельных агентов сети, способных инициировать связи, приводящие, возможно к временному, но появлению новых кластеров в результате объединения уже имеющихся;
- ограничение функциональной возможности, направленной на создание новых связей, агентов, состоящих в кластерной структуре с максимальным числом агентов.

Предложенный подход позволяет существенно повысить информационную безопасность и устойчивость предпринимательской сети в целом к потенциальным угрозам через выделение и усиление информационной защиты наиболее важных и значимых агентов сети не с позиции их формального положения и статуса в структуре, а с позиции их потенциальной угрозы для всей сети в случае атаки или взлома.

Вопрос информационной безопасности соединений различной природы является приоритетным и требует индивидуального подхода, так как методы защиты, используемые в глобальной сети, в первую очередь, ориентированы на поддержание стабильной работы сети в целом. В то время как информационная безопасность отдельно взятых соединений зависит не только от методов защиты, но и от природы данного соединения, которая априори отражается в целеполагании потенциальной угрозы.

Соответственно, предложенный подход по мониторингу потенциально привлекательных агентов сети с позиции внешнего влияния не является универсальным, но сам алгоритм может быть использован при разработке соответствующих индивидуальных методик для оценки информационной безопасности, или целостности сетей различной природы, представимой в виде ориентированного графа и наложении соответствующих характеристик на его связи.

**Библиографический список:**

1. Асаул А.А. Методологические аспекты формирования и развития предпринимательских сетей. – СПб.: «Гуманистика», 2004. – 256 с.
2. Шерешева М.Ю. Формы сетевого взаимодействия компаний. М.: Изд. дом ГУ–ВШЭ, 2010. – 339 с.
3. Жаркова Е.С. Экономические теории размещения производства: от штандорта к кластерам // Вестник СПбГУ. – 2011. – Сер. 5. – Вып. 1. – С. 145–150.
4. Уильямсон О. Экономические институты капитализма: фирмы, рынки, «отношенческая» контрактация. – СПб.: Лениздат, 1996. – 702 с.
5. Радаев В.В. Рынок переплетение социальных сетей // Российский журнал менеджмента. – 2008. – Т.6. – №2. – С. 47–54.
6. Granovetter M. Business Groups. The Handbook of Economic Sociology. – N.Y., 1994.
7. Катькало В.С. Межфирменные сети: проблематика исследований новой организационной категории в 1980–90е гг. // Вестник СПбГУ. Сер.5: Экономика. – 1999. – № 2. – С. 21–38.
8. Elfring T., Hulsink W. Networks in entrepreneurship: The case of high-technology firms // Small Business Economics. – 2001. – Vol. 21(4). – P. 409–422.
9. Davidsson P., Honig B. The role of social and human capital among nascent Entrepreneurs // Journal of Business Venturing. – 2003. – Vol. 18(3). – P. 301–331.

10. Erdos P., Renyi A. On random graphs // Publicationes Mathematica. – 1959. – Vol. 6. – P. 290–297.
11. Newman M.E. The structure and function of complex networks. – SIAM Review, 2003.
12. Леш А. Пространственная организация хозяйства. – М.: Наука, 2007. – 663 с.
13. Штульберг Б.М., Введенский В.Г. Региональная политика России: теоретические основы, задачи и методы реализации. – М.: Гелиос АРВ, 2009. – 208 с.
14. Marshall A. Principles of Economics. Variorum edition overseen be C. Guillebaud. – L.: McMillan Press, 1961. – 450 p.
15. Porter M.E. On Competition. – Boston: Harvard Business School Press, 1998. – 485 p.
16. Albert R., Barabasi A. Statistical mechanics of complex networks // Reviews of Modern Physics. – 2002. – Vol. 74. – P. 47–97.
17. Aggarwal C.C. Social Network Data Analytics. – Kluwer Academic Publishers, 2011. – 502 p.
18. Everton S.F. Disrupting Dark Networks (Structural Analysis in the Social Sciences). – Cambridge University Press, 2012. – 482 p.
19. Асаул А.А. Организация предпринимательской деятельности. – Москва: Проспект, 2016. – 400 с.
20. Tsitsiashvili G., Bulgakov V., Osipova M., Losev A., Kharchenko Yu. Construction of subgraph from graph shortest way//Applied Mathematical Sciences. – 2015. – Vol. 79(9). – P. 3911–3918.

**References:**

1. Asaul A.A. Methodological aspects of the formation and development of entrepreneurial networks. SPb.: «*Gumanistika»*, 2004: 256. (In Russ)
2. Sheresheva M.Yu. Forms of network interaction of companies. M.: Izd. dom GU–VShE`, 2010: 339. (In Russ)
3. Zharkova E.S. Economic theories of production location: from standort to clusters. [Vestnik SPbGU ] *Bulletin of St. Petersburg State University*, 2011; 5(1): 145–150. (In Russ)
4. Uil`yamson O. Economic institutions of capitalism: firms, markets, "relational" contracting. *SPb.: Lenizdat*, 1996: 702. (In Russ)
5. Radaev V.V. The market for the interweaving of social networks. *Rossijskij zhurnal menedzhmenta*, 2008; 6(2): 47–54 (In Russ)
6. Granovetter M. Business Groups. *The Handbook of Economic Sociology. N.Y.*, 1994.
7. Kat`kalo V.S. Interfirm Networks: Research Issues of a New Organizational Category in the 1980–90s. [Vestnik SPbGU Bulletin of St.] *Petersburg State University*. Ser.5: E`konomika, 1999; 2:21–38. (In Russ)
8. Elfring T., Hulsink W. Networks in entrepreneurship: The case of high-technology firms. *Small Business Economic*s. 2001; 21(4): 409–422.
9. Davidsson P., Honig B. The role of social and human capital among nascent Entrepreneurs. *Journal of Business Venturing*. 2003; 18(3): 301–331.
10. Erdos P., Renyi A. On random graphs. *Publicationes Mathematica*. 1959; 6: 290–297.
11. Newman M.E. The structure and function of complex networks. *SIAM Review*, 2003.
12. Lesh A. Spatial organization of the economy. M.: *Nauka*, 2007: 663. (In Russ)
13. Shtul`berg B.M., Vvedenskij V.G. Regional Policy of Russia: Theoretical Foundations, Tasks and Methods of Implementation. *M.: Gelios ARV*, 2009: 208. (In Russ)
14. Marshall A. Principles of Economics. Variorum edition overseen be C. Guillebaud. *L.: McMillan Press*, 1961: 450.
15. Porter M.E. On Competition. Boston: *Harvard Business School Press*, 1998: 485.
16. Albert R., Barabasi A. Statistical mechanics of complex networks. *Reviews of Modern Physics*, 2002; 74: 47–97.
17. Aggarwal C.C. Social Network Data Analytics. *Kluwer Academic Publishers*, 2011: 502.
18. Everton S.F. Disrupting Dark Networks (Structural Analysis in the Social Sciences). *Cambridge University Press*, 2012: 482.
19. Asaul A.A. Organization of entrepreneurial activity. Moskva: *Prospekt*, 2016. 400 p. (In Russ)
20. Tsitsiashvili G., Bulgakov V., Osipova M., Losev A., Kharchenko Yu. Construction of subgraph from graph shortest way. *Applied Mathematical Sciences*, 2015; 79(9): 3911–3918.

**Сведения об авторе:**

Александр Сергеевич Лосев, кандидат физико-математических наук, старший научный научно-исследовательской группы вероятностных методов и системного анализа; A.S.Losev@yandex.ru

**Information about author:**

Aleksandr S. Losev, Cand. Sci. (Physics and Mathematics), Senior Researcher of the Research Group of Probabilistic Methods and System Analysis; A.S.Losev@yandex.ru

**Конфликт интересов/Conflict of interest.**

Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.

**Поступила в редакцию/Received** 30.04.2022.

**Одобрена после рецензирования/ Reviced** 23.05.2022.

**Принята в печать/Accepted for publication** 23.05.2022.