МОДЕЛИРОВАНИЕ СЕТЕВОЙ ИНФРАСТРУКТУРЫ СЛОЖНЫХ ОБЪЕКТОВ ДЛЯ РЕШЕНИЯ ЗАДАЧИ ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

Лаврова Д.С.[1], Зегжда Д.П.[2], Зайцева Е.А.[3]

Аннотация. *В данной статье авторы предлагают подход к моделированию сетевой инфраструктуры сложных крупномасштабных объектов, в том числе, критического назначения, с использованием теории графов.*

***Целью** исследования является разработка математической модели сетевой инфраструктуры сложных крупномасштабных объектов, позволяющей формализовать целевую функцию объекта и кибератаки, направленные на нарушение его целевой функции.*

***Метод** исследования заключается в представлении сетевой инфраструктуры сложного объекта в виде ориентированного графа, в описании целевой функции как множества маршрутов на графе и систематизации кибератак в виде унарных операций над графом.*

***Результатом** исследования является графовая модель, описывающая сетевую инфраструктуру сложных крупномасштабных объектов с учетом выполняемой ими целевой функции. Представлены различные типы целевых функций, описаны кибератаки на сетевую инфраструктуру объектов. Полнота разработанной графовой модели подтверждается сформулированной и доказанной теоремой. Результаты исследования необходимы для математической постановки задачи предотвращения кибератак на сетевую инфраструктуру сложных крупномасштабных объектов, в том числе, критического назначения.*

Ключевые слова: *предотвращение атак, кибератака, теория графов, целевая функция.*

DOI: *10.21681/2311-3456-2019-2-13-20*

Введение

Последние несколько лет в мире наблюдается значительный рост числа киберугроз, направленных на объекты критической инфраструктуры, вызванный их интеграцией с информационными технологиями [1]. Вектор атак сместился в сторону от нарушения целостности, доступности и конфиденциальности информации к деструктивным воздействиям на компоненты технологической инфраструктуры, нарушающим корректность ее функционирования. Последствия таких воздействий могут быть катастрофическими. Деструктивным кибервоздействиям подвергаются информационные структуры различного назначения: военные организации [2, 3], финансовые институты [4-6], отрасли электроэнергетики [7, 8], транспорта [9, 10] и т.д. При этом, следует отметить, что многие объекты критической инфраструктуры реализуют необратимые физические процессы (что характерно, например, для атомной и энергетической отраслей), в связи с чем развитие ряда кибератак, которые не были обнаружены на ранней стадии, не удастся остановить.

Значимость обеспечения безопасности критических объектов повлекла за собой развитие методов оценки рисков таких объектов [11-13]. Однако в подобных исследованиях внимание в основном уделяют уже известным типам угроз, в то время как методы, применяемые злоумышленниками, совершенствуются [14].

В таких условиях актуальной является задача предотвращения кибератак [15, 16], ее можно разделить на два этапа:

раннее предупреждение кибератак, в рамках этого этапа происходит прогнозирование кибератак, их раннее обнаружение и локализация;

противодействие кибератакам, в рамках данного этапа в структуру защищаемой системы или сети вносится ряд изменений, делающих невозможным реализацию кибератаки.

В статье представлена формальная постановка задачи предотвращения кибератак на сетевую инфраструктуру сложных крупномасштабных объектов. В рамках данной задачи с использованием теории графов выполнено моделирование сетевой инфраструктуры, включающее описание целевой функции объекта и систематизацию кибератак. Также авторами доказана теорема о полноте предложенной графовой модели.

Актуальность рассмотрения именно сетевой инфраструктуры подчеркивается географической распределенностью технологических объектов (крупных заводов, медицинских учреждений и т.д.) и тенденцией к развитию сетевой инфраструктуры при создании «умных» цифровых промышленных предприятий. Например, японская компания химической промышленности Sumitomo Chemical создает «цифровые заводы» – производственные предприятия нового поколения, функционирующие

1 Лаврова Дарья Сергеевна, кандидат технических наук, доцент, Санкт-Петербургский политехнический университет Петра Великого (СПбПУ), Санкт-Петербург, Россия. E-mail: lavrova@ibks.spbstu.ru.

2 Зегжда Дмитрий Петрович, доктор технических наук, профессор, Санкт-Петербургский политехнический университет Петра Великого (СПбПУ), Санкт-Петербург, Россия. E-mail: dmitry@ibks.spbstu.ru.

3 Зайцева Елизавета Алексеевна, аспирант, Санкт-Петербургский политехнический университет Петра Великого (СПбПУ), Санкт-Петербург, Россия. E-mail: eaz@ibks.spbstu.ru.

и управляемые посредством реализации концепции Интернета вещей, начиная с построения концептуально новой сетевой инфраструктуры управления заводом с использованием решений японской компании NEC, одной из крупнейших мировых телекоммуникационных компаний [17]. Особенное внимание сетевой инфраструктуре было уделено и при цифровизации одного из наиболее престижных медицинских учреждений Японии – Университетской клиники Кейо [18].

Математическая постановка задачи предотвращения кибератак в части представления защищаемой сетевой инфраструктуры и систематизации кибератак представляет собой научный задел для разработки методов и средств противодействия кибератакам, что, в соответствии со Стратегией НТР РФ, является одним из приоритетов.

1. Постановка задачи в виде моделирования сетевой инфраструктуры сложных объектов с использованием теории графов

Вся сетевая инфраструктура моделируется в виде ориентированного графа G, где множество вершин $V=\{v_1,...,v_N\}$ представляет все устройства сети, а множество дуг $E=\{e_1,...,e_M\}$ характеризует все возможные связи между устройствами, проявляющиеся как обмен информхацией.

Каждое устройство сети, представляемое вершиной v_i графа G, характеризуется набором функций, которое оно способно выполнять: $f(v_i)=\{f_{vi}^{(1)},f_{vi}^{(2)},...,f_{vi}^{(k)}\}$. Описание устройств сети через выполняемые ими функции, а не через тип устройства, определяет целевую функцию F сети, которая может заключаться в передаче данных от начального узла к конечному, или в передаче данных определенным маршрутом, или характеризоваться выполняемыми преобразованиями над данными. В любом случае, такая функция может быть представлена как маршрут на графе, где посещение вершин инициирует выполнение определенной функции этой вершиной.

Поскольку на первый план здесь выходит именно последовательное выполнение функций устройствами сети, то, помимо маршрута на графе, целевая функция F может быть представлена как множество суперпозиций функций. Суперпозиция функций представляет собой применение одной функции к результату другой. При этом, за выполнение целевой функции отвечает множество компонентов КФС, описываемых в терминах графовой модели множеством вершин V^'. Одно и то же устройство $v_i \in V'$ может реализовывать как одну, так и несколько функций, входящих в суперпозицию F, причем не обязательно эти функции будут следовать друг за другом.

Каждая дуга (направленное ребро) e_{ij} графа G обладает некоторой характеристикой $\omega_{e_{ij}}$, которая может иметь различный смысл в зависимости от типа сети (например, $\omega_{e_{ij}}$ может характеризовать скорость канала передачи данных между устройствами, представленными на графе вершинами v_i и v_j).

В терминах графовой модели, целевая функция системы F_G может быть выражена любым из следующих способов:

1. Маршрут на графе G, с последовательным посещением вершин, реализующих необходимые функции: $F_G=f_k \circ f_{k-1} \circ ... \circ f_1$. Здесь реализация целевой функции сети определяется применением функции f_k к результату функции f_{k-1}, и так далее – рекурсивно, где началом является функция f_1. На рис. 1 а) представлен граф сети для такого случая: целевая функция реализуется путем последовательного посещения вершин 1-2-4-8-10-13-11-14.

2. Множество маршрутов на графе, имеющих общие вершины. Подобное отображение целевой функции характерно для сетей, интегрированных со сложными промышленными объектами, где для реализации каким-либо компонентом требуются данные, полученные в результате взаимодействия множества компонентов. Тогда целевая функция описывается суперпозицией $F_G=(f_k \circ f_{k-1} \circ ... \circ f_1)$, где $\exists f_i \in F_G: f_i=f_j \circ f_{j-1} \circ ... \circ f_l$, где $f_j,f_{j-1},...,f_l \notin F_G$. В представленном примере (рис. 1 б)) вершинам 1, 8, 10 и 13 требуются дополнительные данные для выполнения функций в рамках реализации КФС технологического процесса, являющегося целевой функцией системы. В частности, вершине 1 требуются данные от вершин 3 и 5, вершина 8 является частью маршрута 7-6-8, для выполнения своих функций вершине 10 требуются данные от вершины 9, а вершине 13 – данные от вершины 12. Такие дополнительные маршруты обозначены пунктиром.

3. Множество независимых маршрутов. От варианта 2 такой способ отличается тем, что у маршрутов нет общих точек. Как правило, часть таких маршрутов направлена на контроль параметров реализации технологического процесса (например, таким может быть процесс поддержания температуры, необходимой для плавления металла и последующего изготовления деталей из него, контролируемый датчиками, объединенными в сенсорную сеть). В таком случае целевая функция описывается набором суперпозиций функций: $F_G=F_G^{(1)} \cup F_G^{(2)} \cup ... \cup F_G^{(n)}=((f_k \circ f_{k-1} \circ ... \circ f_1),(f_t \circ f_{t-1} \circ ... \circ f_l),...,(f_m \circ f_{m-1} \circ ... \circ f_n))$, при этом, $F_G: \forall i,j \nexists v_k: v_k \in F_G^i, v_k \in F_G^j$, то есть, не существует такой вершины, которая была бы одновременно задействована в более чем одном процессе. В примере (рис. 1 в)) маршруты, характеризующие контроль за выполнением технологического процесса, обозначены пунктиром.

4. Гибридный вариант без циклов – сочетает в себе все вышеописанные варианты, при этом, отсутствуют ограничения на использование каждой вершины только 1 раз: $F_G=F_G^{(1)} \cup F_G^{(2)} \cup ... \cup F_G^{(n)}=((f_k \circ f_{k-1} \circ ... \circ f_1),(f_t \circ f_{t-1} \circ ... \circ f_l),...,(f_m \circ f^{m-1}) \circ ... \circ f_n))$, где $\exists f_i \in F_G: f_i=f_j \circ f_{j-1} \circ ... \circ f_l$, где $f_j,f_{j-1},...,f_l \notin F_G$. Пример представлен на рис.1 г). Здесь присутствуют 2 маршрута, выполняющиеся параллельно маршруту, реализующему целевую функцию сети: 6-7 и 9-12. Также присутствуют маршруты, обеспечивающие данными узлы сети, задействованные в реализации целевой функции: 1-4 и 1-3-5-8. Все дополнительные и «контролирующие» маршруты обозначены пунктиром.

Следует отметить, что любой из вышеописанных вариантов представления целевой функции может

7 Данные Европейско-Средиземноморского сейсмологического центра. Источник: Мировой Центр Данных по физике твердой Земли, Москва (www.wdcb.ru).

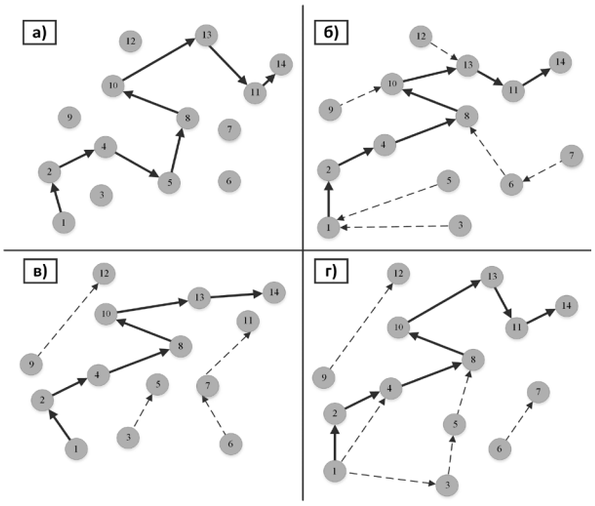

Рис. 1. Графовое представление целевой функции сети

быть усложнен добавлением минимум одного цикла. Цикличность может возникать при автоматической оценке качества реализации сетью ее целевой функции.

Необходимость моделирования целевой функции сложных промышленных объектов связана с тем, что объект должен быть способен сохранять киберустойчивость – способность к реализации своей целевой функции даже в условиях кибератак [1]. Моделирование целевой функции в виде множества маршрутов на графе и представление ее как суперпозиции функций, реализуемых устройствами сети, дает возможность для противодействия кибератаке путем внесения изменений в текущую конфигурацию сети. Наибольшей эффективности при использовании данного подхода достигнут сложные объекты с гибкой организацией сетевой инфраструктуры, например, на базе программно-конфигурируемых сетей [19, 20].

2. Представление кибератак в терминах графовой модели

Рассмотрим сеть, описываемую ориентированным графом G и реализующую целевую функцию F, представляющую собой набор рабочих маршрутов на графе $R=\{S_{ij}\}$. Функция F реализуется с показателем качества Q, значение которого лежит в заданных пределах $[Q_{min};Q_{max}]$.

При реализации злоумышленником кибератак, представляющих собой возмущающие воздействия Z, над графом G выполняются преобразования. При этом, эти преобразования могут быть одного из двух типов:

1) структурные – унарные операции над графом;

2) функциональные – изменения параметров вершин и ребер.

2.1. Структурные преобразования над графом, представляющие собой унарные операции

Определим типы структурных возмущающих воздействий, выражаемых унарными операциями, с использованием теории графов (табл.1). Необходимо отметить, что некоторые унарные операции характерны именно для гиперграфа.

Определение. Гиперграфом $H=(X,U;R)$ называется пара множеств $X=\{x_i|i\in I\}$, $U=\{u_j|j\in J\}$ вместе с двуместным предикатом $R\Leftrightarrow R(x,u)$, определенным при всех $x\in X$, $u\in U$. Элементы $x\in X$ называются вершинами, элементы $u\in U$ ребрами, а предикат R инцидентором гиперграфа H; вершина x инцидентна или не инцидентна ребру u в H, смотря по тому, истинно или ложно для них высказывание R(x,u).

Свойства гиперграфа:

Одним ребром может соединяться не пара вершин, а множество вершин.

Каждому ребру инцидентно одинаковое количество вершин.

2.2. Функциональные преобразования над графом, заключающиеся в изменениях параметров вершин и ребер

Таблица 1.

Возмущающие воздействия Z, отражаемые унарными операциями

Унарная операция	Воздействие на граф в результате применения операции	Пример атаки, выражающейся как такое изменение в графе
1. Удаление вершины v_i из графа G, получение нового графа G^’	Удаляется вершина и все инцидентные ей ребра (дуги): G=<V,E>, G’=<V’,E’>, V’=V\{v_i},E’ ⊆E	Атака отказа в обслуживании (DoS), отключение устройства или вывод его из строя.
2. Добавление вершины v_i к графу G, получение нового графа G’	Добавляется изолированная вершина к графу (орграфу), новых ребер (дуг) не появляется G=<V,E>, G’=<V’,E’>,V’=V ∪{v_i}, E’=E	Добавление злоумышленником устройства, выдающего себя за легитимное.
3. Удаление ребра (дуги) e_{ij} из графа G, получение нового графа (орграфа) G’	Удаляется только ребро (дуга) e_{ij}, вершины v_i,v_j остаются: G=<V,E>, G’=<V’,E’>,V’=V,E’=E\\{e_{ij}}	Изменение правил работы или настроек системы, запрещающие общение устройства с каким-либо другим

4. Добавление дуги e_ij, получение нового графа G^’	G=<V,E>, G’=<V’,E’>,V’=V, E’=E ∪{e_{ij}}	Изменение правил работы или настроек системы, инициирующие общение устройства с каким-либо другим
5. Сильное удаление вершины v_i из гиперграфа G	Удаляется вершина и все инцидентные ей ребра (дуги): G=<V,E;R>, G’=<V’,E’,R’>, V’=V\{v_i}, E’=E\{e|R(v_i,e)≡1}	Атака DoS, отключение устройства или вывод его из строя повлекшая за собой изменение правил работы или настроек системы, запрещающее общение группы устройств друг с другом
6. Слабое удаление вершины v_i из гиперграфа G	Удаляется вершина, а все инцидентные ей ребра (дуги) остаются: G=<V,E;R>, G’=<V’,E,R’>, V’=V\{v_i}	Атака DoS, отключение устройства или вывод его из строя
7.Сильное удаление дуги e из гиперграфа G	Удаляется дуга и все инцидентные ей вершины: G=<V,E;R>, G’=<V’,E’,R’>, V’=V\{v_i |R(v_i,e)≡1}, E’=E\{e}	Изменение правил работы или настроек системы, запрещающее общение группы устройств друг с другом с последующим выводом данной группы устройств из строя
8. Слабое удаление дуги e из гиперграфа G	Удаляется только дуга e_{ij}, вершины v_i,v_j остаются: G=<V,E,>, G’=<V,E’,R’>, E’=E\\{e_{ij}}	Изменение правил работы или настроек системы, запрещающее общение группы устройств друг с другом
9. Замыкание (слияние или отождествление), получение нового графа (орграфа) G’	Пара вершин v_i,v_j в графе G замыкаются (отождествляются), если они заменяются такой новой вершиной v_k, что все дуги в графе (орграфе) G, инцидентные v_i и v_j, становятся инцидентыми новой вершине v_k G’=<V’,E’>, V’=(V\{v_i,v_j})∪{v_k} E’ ⊆ E	Атака «воронка» (Sinkhole), характерная для беспроводных сенсорных сетей. Скомпрометированный узел сети «слушает» запросы на маршруты и отвечает сенсорным узлам, что «знает» кратчайший маршрут до базовой станции.
10. Транзитивное замыкание орграфа (добавление дуг к орграфу и получение транзитивного орграфа)	G=(V,E) G’=(V,E’) E’=E∪U U:∀e_{ij}∈E∪U,e_{jk}∈E∪U ∃e_{ik}∈E∪U	Изменение правил работы или настроек системы, инициирующие прямое общение устройств с устройствами, общение с которыми раньше было только косвенным
11. Стягивание – удаление дуги и отождествление его концевых вершин, получение нового графа G^’	Из графаG удаляется дуга e_{ij}, а вершины v_i,v_j заменяются такой новой вершиной v_k, что все дуги в графе (орграфе) G, инцидентные v_i и v_j, становятся инцидентыми новой вершине v_k: G’=<V’,E’>,V’=(V\{v_i,v_j})∪{v_k}, E’=E\\{e_{ij}}	Сложная атака, сочетающая в себе атаку «воронки» и запрет соединения между узлами
12. Подразбиение дуги (внесение в дугу новой вершины), получение нового графа G’	К графу G добавляется новая вершина v_k, дуга e_{ij} удаляется, добавляются дуги e_{ik} и e_{kj} G’=<V’,E’>, V’=V ∪ {v_k} E’=(E\\{e_{ij}})∪ {e_{ik},e_{kj}}	Атака «человек посередине» (Man-in-the-Middle, MITM), вмешательство злоумышленника в процесс передачи данных, перехват данных

В соответствии с графовой моделью сети, каждая вершина v_i графа G описывается кортежем <id,type,P_{vi},F_{vi}>. – множество параметров вершины, $F_{v_i} = \left\{f_{v_{i_1}}^m, f_{v_{i_2}}^m, \dots\right\}$ – множество функций, поддерживаемых узлом, где индекс m обозначает режим выполнения функции (использует ли данный узел функциональность $f_{V_{ij}}$ в текущем процессе или нет). Множество $\Omega_{ij}=\{\omega_{ij},\omega_{ik},\dots\}$ характеризует параметры дуг графа G.

Тогда изменения, вносимые злоумышленником, могут влиять на:

1) P_{vi} – множество параметров вершины, меняются значения параметров;

2) F_{vi} – множество параметров функций:

изменение режима выполнения функции, проявляющегося как изменение значения m с 0 на 1 и наоборот (узел раньше использовал эту функциональность в текущем процессе, а теперь перестал, и наоборот)

изменение числа реализуемых в данном процессе функций – удаление/добавление функций, которые данный узел способен реализовывать.

Ω_{ij} – множество параметров дуг графа.

2.3. Теорема о полноте графовой модели

Полноту предложенной графовой модели с точки зрения отражения в ней всех возможных типов кибератак требуется подтвердить формально.

Введем функцию φ, сопоставляющую каждой вершине v_i из множества V список функций, которые данная вершина может реализовать:

$$\varphi:V\rightarrow F \quad (1)$$

Введем функцию γ, сопоставляющую каждой дуге характеристику (или множество характеристик):

$$\gamma:E\rightarrow\Omega \quad (2)$$

Сеть может быть описана с использованием трех матриц:

1) матрица смежности S:s_{ij}=1 if $\exists\, e_k=(v_i,v_j),e_k\in E,s_{ij}$=0 otherwise (где if – условный оператор, a otherwise означает «в противном случае»);

2) матрица функций вершин VF:vf_{ij}=1 if $f_j\in\varphi(v_i),vf_{ij}$=0 otherwise;

3) матрица характеристик для дуг EΩ: $e\omega_{ij}$=1 if $\omega_j\in\gamma(e_i),e\omega_{ij}$=0 otherwise.

Теорема о полноте графовой модели

Для доказательства теоремы рассмотрим возможные объекты кибератак в терминах графовой модели. Очевидно, что объектом кибератаки может стать либо некоторое множество вершин графа, либо множество дуг, либо некоторое множество вершин и дуг. В каждом из трех случаев изменения могут коснуться либо числа вершин/дуг, либо их характеристик, либо и того, и того.

Тогда любое изменение, произошедшее в сети, может быть отражено при помощи представленных выше трёх матриц:

1) изменения в топологии сети отразятся в матрице смежности S, поскольку приведут к изменению числа устройств и/или связей между ними;

2) изменение в работе устройства (например, активация программных закладок) отразится на множестве выполняемых им функций, что повлечет за собой преобразование матрицы функций VF;

3) изменения во взаимодействии устройств (например, снижение скорости передачи канала данных) отразятся в матрице характеристик EΩ.

Тогда доказательство теоремы сводится к доказательству четырёх утверждений.

Утверждение 1: Изменение, касающееся количества вершин V графа, приведет к изменению матриц S и VF.

Утверждение 2: Изменение, касающееся параметров вершин V графа (выполняемых ими функций из множества F), ведет к изменению матрицы VF.

Утверждение 3: Изменение, касающееся количества дуг E графа, ведет к изменению матриц S, EΩ.

Утверждение 4: Изменение, касающееся параметров дуг (характеристик дуг из множества Ω), ведет к изменению матрицы EΩ.

Доказательство утверждения 1

Докажем от противного. Допустим, что это не так, и изменения множества вершин не отражаются хотя бы на одной из указанных матриц. Тогда необходимо рассмотреть несколько случаев:

1. Изменение количества вершин не отражается на матрице S.

Пусть в графе появилась новая вершина v_i, способна выполнять множество функций $\{f_k\}$. v_i первоначально не имеет связей с другими вершинами. Матрица S по определению должна содержать нули в позициях (i,j), если вершины v_i и v_j не являются смежными. Таким образом, в матрицу S будет добавлена новая строка, и изменение отразится на матрице S. Получено противоречие.

Пусть из графа удаляется вершина v_i, обладающая множеством функций $\{f_k\}$. v_i является смежной или несмежной по отношению к каждой из вершин. Матрица S по определению должна содержать нули в позициях (i,j), если вершины v_i и v_j не являются смежными, и единицы, если вершины являются смежными. При удалении вершины данная информация станет недействительной и будет удалена из матрицы S. Матрица S изменилась, получено противоречие.

2. Изменение количества вершин не отражается на матрице VF.

Пусть в графе появилась новая вершина v_i, обладающая множеством функций $\{f_k\}$. Матрица VF по определению должна содержать 1 в позиции (i,j), если вершина v_i обладает функцией f_j. Поэтому при добавлении вершины в граф, в матрицу VF будет добавлена новая строка. Матрица VF изменилась, получено противоречие.

Пусть из графа удаляется вершина v_i, обладающая множеством функций $\{f_k\}$. Матрица VF по определению должна содержать ноль в позиции (i,j), если вершина v_i не обладает функцией f_j, и единицу, если вершина функцией обладает. При удалении вершины данная информация станет недействительной и будет удалена из матрицы VF. Матрица VF изменилась, получено противоречие.

Доказательство утверждения 2

Докажем от противного. Допустим, что это не так, и изменения множества параметров вершин не отражаются на указанной матрице.

Пусть вершина v_i, обладающая множеством функций $\{f_k\}$, получает способность выполнять новую функ-

цию f_j. Поскольку раньше вершина не обладала данной функцией в позиции (i,j), матрица VF содержит ноль. По определению матрицы VF, если вершина v_i обладает функцией f_j, позиция (i,j) матрицы VF должна содержать единицу. Поэтому при добавлении новой функции какой-либо вершине будет изменено одно из значений в матрице VF, следовательно, получено противоречие.

Пусть вершина v_i, обладающая множеством функций $\{f_k\}$, лишается способности выполнять функцию f_j. Поскольку раньше вершина обладала данной функцией, в ячейке (i,j) матрицы VF стоит 1. По определению матрицы VF, если вершина v_i не обладает функцией f_j, позиция (i,j) матрицы VF должна содержать значение 0. Поэтому при удалении одной из функций у вершины в матрице VF будет изменено одно из значений, следовательно, получено противоречие.

Доказательство утверждения 3

Докажем от противного. Допустим, что это не так, и изменения множества дуг не отражаются хотя бы на одной из указанных матриц. Тогда необходимо рассмотреть несколько случаев.

1. Изменение количества дуг не отражается на матрице S.

Пусть в графе появилась новая дуга, обладающая множеством характеристик $\{\omega_k\}$. Любая дуга связывает некоторые вершины, то есть, делает их смежными. Пусть эта дуга появилась между вершинами v_i и v_j. До появления новой дуги матрица S содержала значение 0 в позиции (i,j). После добавления дуги матрица S по определению должна содержать 1 в позиции (i,j), так как вершины v_i и v_j теперь являются смежными. Следовательно, получено противоречие.

Пусть из графа удаляется дуга $e_k=(v_i,v_j)$, обладающая множеством характеристик $\{\omega_k\}$. Матрица S по определению должна содержать 1 в позиции (i,j), так как вершины v_i и v_j являются смежными. При удалении дуги вершины перестанут быть смежными, значит, матрица S изменит одно из своих значений. Следовательно, получено противоречие.

2. Изменение количества ребер не отражается на матрице EΩ.

Пусть в графе появилась новая дуга e_i, обладающая множеством характеристик $\{\omega_k\}$. Матрица EΩ по определению должна содержать единицы в позициях (i,j), если дуга e_i обладает характеристикой ω_j. Поэтому при добавлении дуги в матрицу EΩ будет добавлена новая строка. Следовательно, получено противоречие.

Пусть из графа удаляется дуга e_i, обладающая множеством характеристик $\{\omega_k\}$. Матрица EΩ по определению должна содержать ноль в позиции (i,j), если дуга e_i не обладает характеристикой ω_j, и единицу, если обладает. Таким образом, в случае неизменности матрицы при удалении дуги, информация в ячейках матрицы станет недействительной. Следовательно, получено противоречие.

Доказательство утверждения 4

Докажем от противного. Допустим, что это не так, и изменения множества параметров дуг не отражаются на указанной матрице.

Пусть дуга e_i, обладающая множеством характеристик $\{\omega_k\}$, получает новую характеристику ω_j. Поскольку раньше дуга не обладала данной характеристикой, в позиции (i,j) матрица EΩ содержит 0. По определению матрицы EΩ, если дуга e_i обладает характеристикой ω_j, позиция (i,j) матрицы EΩ должна содержать 1. Поэтому при добавлении дуге новой характеристики, в матрице EΩ будет изменено одно из значений. Следовательно, получено противоречие.

Пусть дуга e_i, обладающая множеством меток $\{\omega_k\}$, лишается характеристики ω_j. Поскольку раньше дуга обладала данной характеристикой, в позиции (i,j) матрица EΩ содержит 1. По определению матрицы EΩ, если дуга e_i не обладает характеристикой ω_j, позиция (i,j) матрицы EΩ должна содержать 0. Поэтому при удалении одной из характеристик у дуги в матрице EΩ будет изменено одно из значений. Следовательно, получено противоречие.

Все сформулированные утверждения доказаны, что позволяет говорить о доказательстве теоремы о полноте графовой модели. Разработанная графовая модель является научным заделом для создания технологии предотвращения кибератак, поскольку в терминах теории графов могут быть описаны не только кибератаки, но и возможные сценарии противодействия им, реализуемые за счет внесения изменений в структуру графа. За счет эффективного выполнения таких преобразований, сохраняющих способность объекта к реализации своей целевой функции, будет обеспечено упреждающее воздействие, не позволяющее злоумышленнику реализовать кибератаку.

Выводы

В статье представлена формализация сетевой инфраструктуры сложных крупномасштабных объектов в виде графовой модели. Сетевая инфраструктура была представлена в виде ориентированного графа, на котором также определена целевая функция объекта. Формализация понятия целевой функции для сложных объектов особенно актуальна в связи с цифровизацией технологической инфраструктуры и переходом от информационных систем к киберфизическим системам, реализующих физические процессы путем сетевого обмена данными между устройствами системы.

Для таких объектов способность выполнения целевой функции даже в условиях кибератак является важнейшей задачей. Представление целевой функции в виде множества маршрутов на графе в совокупности с систематизацией кибератак на основе унарных операций над графом позволило математически описать часть задачи предотвращения кибератак. Авторами доказана полнота разработанной графовой модели с точки зрения деструктивных кибервоздействий на сетевую инфраструктуру сложных объектов, в том числе, критического назначения.

Исследование выполнено в рамках гранта Президента РФ для государственной поддержки ведущих научных школ Российской Федерации НШ-2992.2018.9 (соглашение 075-02-2018-504).

Рецензент: *Сикарев Игорь Анатольевич, доктор технических наук, профессор Государственного университета морского и речного флота имени адмирала С.О. Макарова, Москва, Россия. E-mail: sikarev@yandex.ru*

Литература

1. Zegzhda D. P., Pavlenko E. Y. Cyber-physical system homeostatic security management //Automatic Control and Computer Sciences. – 2017. – №. 8 (51). – С. 805-816.
2. Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. – 2019. – №. 1 (29). – С. 2-9.
3. Бородакий Ю.В., Добродеев А.Ю., Нащекин П.А., Бутусов И.В. О подходах к реализации централизованной системы управления информационной безопасностью АСУ военного и специального назначения // Вопросы кибербезопасности. 2014. №. 2 (3). С. 2-9.
4. Шеремет И. А. Направления подготовки специалистов по противодействию киберугрозам в кредитно-финансовой сфере // Вопросы кибербезопасности. 2016. №. 5 (18). С. 2-7.
5. Малюк А. А. Организационно-методические проблемы обнаружения атак на объекты информационной инфруструктуры кредитно-финансовой сферы // Вопросы кибербезопасности. 2016. №. 5 (18). С. 8-14.
6. Ревенков П. В., Бердюгин А. А. Расширение профиля операционного риска в банках при возрастании DDoS-угроз // Вопросы кибербезопасности. 2017. №. 3 (21). С. 16-23.
7. Массель Л. В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. №. 4 (17). С. 2-10.
8. Колосок И. Н., Гурина Л. А. Повышение кибербезопасности интеллектуальных энергетических систем методами оценивания состояния // Вопросы кибербезопасности. 2018. №. 3 (27). С. 63-69.
9. Бакуркин Р. С., Безродный Б. Ф., Коротин А. М. Противодействие компьютерным атакам в сфере железнодорожного транспорта // Вопросы кибербезопасности. 2016. №. 4 (17). С. 29-35.
10. Косьянчук В.В., Сельвесюк Н.И., Зыбин Е.Ю., Хамматов Р.Р., Карпенко С.С. Концепция обеспечения информационной безопасности бортового оборудования воздушного судна // Вопросы кибербезопасности. 2018. №. 4 (28). С. 9-20.
11. Братченко А. И., Бутусов И.В., Кобелян А.М., Романов А.А. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления // Вопросы кибербезопасности. 2019. №. 1 (29). С. 18-24.
12. Полищук Ю. В. Энтропийный подход к оценке ущерба от реализации угроз безопасности информации больших технических систем // Вопросы кибербезопасности. – 2018. – №. 1 (25). – С. 39-45.
13. Чукляев И. И. Научно-методическое обеспечение комплексного управления рисками нарушения защищенности функционально-ориентированных информационных ресурсов информационно-управляющих систем // Вопросы кибербезопасности. 2016. №. 4 (17). С. 61-71.
14. Мошков А. Н. Новые информационные угрозы требуют идти в ногу со временем // Вопросы кибербезопасности. 2014. №. 3 (4). С. 2-6.
15. Браницкий А. А., Котенко И. В. Открытые программные средства для обнаружения и предотвращения сетевых атак // Защита информации. Инсайд. 2017. №. 3 (75). С. 58-66.
16. Згоба А. И., Маркелов Д. В., Смирнов П. И. Кибербезопасность: угрозы, вызовы, решения // Вопросы кибербезопасности. 2014. №. 5 (8). С. 30-38.
17. Sumitomo Chemical adopts NEC's SDN solutions for the network infrastructure of its Chiba Works // https://www.nec.com/en/press/201711/ global_20171127_02.html
18. NEC uses SDN to develop a network for Keio University Hospital // https://www.nec.com/en/press/201610/global_20161018_01.html
19. Зегжда Д. П., Павленко Е. Ю. Обеспечение киберустойчивости программно-конфигурируемых сетей на основе ситуационного управления // Проблемы информационной безопасности. Компьютерные системы. 2018. №. 1. С. 160-168.
20. Калинин М. О., Павленко Е. Ю. Повышение отказоустойчивости и доступности программно-конфигурируемых сетей с помощью управления сетевым оборудованием на основе метода многокритериальной оптимизации по параметрам качества обслуживания // Проблемы информационной безопасности. Компьютерные системы. 2013. №. 1. С. 33-39.

SIMULATION OF COMPLEX OBJECTS NETWORK INFRASTRUCTURE TO SOLVE THE PROBLEM OF COUNTERACTION TO CYBER ATTACKS

Lavrova D.S.[4], Zegzhda D.P.[5], Zaitceva E.A.[6]

The work was funded by the Russian Federation Presidential grants for support of leading scientific schools (NSh-2992.2018.9) Contract No. 075-02-2018-504.

Abstract. *In this article, the authors propose an approach to modeling the network infrastructure of complex large-scale objects, including critical ones, using graph theory.*

4 Daria Lavrova, Ph.D., Associate Professor, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: lavrova@ibks.spbstu.ru.

5 Dmitrii Zegzhda, Dr.Sc., Professor of RAS, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: dmitry@ibks.spbstu.ru.

6 Zaitceva Elizaveta, Ph.D. student, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: eaz@ibks.spbstu.ru.

The aim of the study is to develop a mathematical model of the network infrastructure of complex large-scale objects, allowing to formalize the target function of the object and cyber attacks aimed at disrupting its objective function.

The research method consists in representing the network infrastructure of a complex object as a directed graph, describing the objective function as a set of routes on the graph, and systematizing cyber attacks in the form of unary operations on the graph.

The result of the study is a graph model describing the network infrastructure of complex large-scale objects, taking into account the objective function performed by them. Different types of target functions are presented, cyber attacks on the network infrastructure of objects are described. The completeness of the developed graph model is confirmed by the stated and proved theorem. The research results are necessary for the mathematical formulation of cyber attacks prevention problem.

Keywords: *attack prevention, graph theory, prediction, cyber-physical systems, cyber-resilience.*

References

1. Zegzhda D. P., Pavlenko E. Y. Cyber-physical system homeostatic security management, Automatic Control and Computer Sciences, 2017, No 8 (51), pp. 805-816.
2. Romashkina N.P. Global'nye voenno-politicheskie problemy mezhdunarodnoj informacionnoj bezopasnosti: tendencii, ugrozy, perspektivy, Voprosy kiberbezopasnosti, 2019, No 1 (29), pp. 2-9.
3. Borodakij YU.V., Dobrodeev A.YU., Nashchekin P.A., Butusov I.V. O podhodah k realizacii centralizovannoj sistemy upravleniya informacionnoj bezopasnost'yu ASU voennogo i special'nogo naznacheniya, Voprosy kiberbezopasnosti, 2014, No 2 (3), pp. 2-9.
4. Sheremet I. A. Napravleniya podgotovki specialistov po protivodejstviyu kiberugrozam v kreditno-finansovoj sfere, Voprosy kiberbezopasnosti, 2016, No 5 (18), pp. 2-7.
5. Malyuk A. A. Organizacionno-metodicheskie problemy obnaruzheniya atak na ob»ekty informacionnoj infrustruktury kreditno-finansovoj sfery, Voprosy kiberbezopasnosti, 2016, No 5 (18), pp. 8-14.
6. Revenkov P. V., Berdyugin A. A. Rasshirenie profilya operacionnogo riska v bankah pri vozrastanii DDoS-ugroz, Voprosy kiberbezopasnosti, 2017, No 3 (21), pp. 16-23.
7. Massel' L. V., Voropaj N.I., Senderov S.M., Massel' A.G. Kiberopasnost' kak odna iz strategicheskih ugroz energeticheskoj bezopasnosti Rossii, Voprosy kiberbezopasnosti, 2016, No. 4 (17), pp. 2-10.
8. Kolosok I. N., Gurina L. A. Povyshenie kiberbezopasnosti intellektual'nyh energeticheskih sistem metodami ocenivaniya sostoyaniya, Voprosy kiberbezopasnosti, 2018, No 3 (27), pp. 63-69.
9. Bakurkin R. S., Bezrodnyj B. F., Korotin A. M. Protivodejstvie komp'yuternym atakam v sfere zheleznodorozhnogo transporta, Voprosy kiberbezopasnosti, 2016, No 4 (17), pp. 29-35.
10. Kos'yanchuk V.V., Sel'vesyuk N.I., Zybin E.YU., Hammatov R.R., Karpenko S.S. Koncepciya obespecheniya informacionnoj bezopasnosti bortovogo oborudovaniya vozdushnogo sudna, Voprosy kiberbezopasnosti, 2018, No. 4 (28), pp. 9-20.
11. Bratchenko A. I., Butusov I.V., Kobelyan A.M., Romanov A.A. Primenenie metodov teorii nechetkih mnozhestv k ocenke riskov narusheniya kriticheski vazhnyh svojstv zashchishchaemyh resursov avtomatizirovannyh sistem upravleniya, Voprosy kiberbezopasnosti, 2019, No 1 (29), pp. 18-24.
12. Polishchuk YU. V. Entropijnyj podhod k ocenke ushcherba ot realizacii ugroz bezopasnosti informacii bol'shih tekhnicheskih sistem, Voprosy kiberbezopasnosti, 2018, No 1 (25), pp. 39-45.
13. Chuklyaev I. I. Nauchno-metodicheskoe obespechenie kompleksnogo upravleniya riskami narusheniya zashchishchennosti funkcional'no-orientirovannyh informacionnyh resursov informacionno-upravlyayushchih sistem, Voprosy kiberbezopasnosti, 2016, No 4 (17), pp. 61-71.
14. Moshkov A. N. Novye informacionnye ugrozy trebuyut idti v nogu so vremenem, Voprosy kiberbezopasnosti, 2014, No 3 (4), pp. 2-6.
15. Branickij A. A., Kotenko I. V. Otkrytye programmnye sredstva dlya obnaruzheniya i predotvrashcheniya setevyh atak, Zashchita informacii. Insajd, 2017, No 3 (75), pp. 58-66.
16. Zgoba A. I., Markelov D. V., Smirnov P. I. Kiberbezopasnost': ugrozy, vyzovy, resheniya, Voprosy kiberbezopasnosti, 2014, No 5 (8), pp. 30-38.
17. Sumitomo Chemical adopts NEC's SDN solutions for the network infrastructure of its Chiba Works, https://www.nec.com/en/press/201711/global_20171127_02.html
18. NEC uses SDN to develop a network for Keio University Hospital, https://www.nec.com/en/press/201610/global_20161018_01.html
19. Zegzhda D. P., Pavlenko E. YU. Obespechenie kiberustojchivosti programmno-konfiguriruemyh setej na osnove situacionnogo upravleniya, Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy, 2018, No 1, pp. 160-168.
20. Kalinin M. O., Pavlenko E. YU. Povyshenie otkazoustojchivosti i dostupnosti programmno-konfiguriruemyh setej s pomoshch'yu upravleniya setevym oborudovaniem na osnove metoda mnogokriterial'noj optimizacii po parametram kachestva obsluzhivaniya, Problemy informacionnoj bezopasnosti. Komp'yuternye sistemy, 2013, No 1, pp. 33-39.