А.В. АНДРЕЕВ, студент гр. КЗИ-109;
Д.В. МИШИН, ст. преподаватель.

АНАЛИТИЧЕСКАЯ ПОДСИСТЕМА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ АСУП

В работе представлена методика выявления элементов информационного процесса корпоративной сети передачи данных. Разработаны алгоритмы удаления и добавления элементов при рассмотрении графа КСПД и ИП КСПД на различных уровнях модели *ISO OSI*. Представлен тестовый расчет.

Ключевые слова: многоуровневая модель, корпоративная сеть передачи данных, элемент, граф, вершина, ребро, информационный процесс, отображение.

Введение. В процессе функционирования автоматизированной системы управления предприятием (АСУП) возможно возникновение некоторых инцидентов связанных с действиями злоумышленника. Анализ большинства инцидентов ИБ требует выявления множества элементов КСПД (которая является информационной инфраструктурой АСУП), задействованных в рассматриваемом ИП. Классической моделью представления КСПД является представление в виде графа [1]. Для достижения поставленной цели КСПД представляется в виде неориентированного графа без петель *G(V, E)*, вершины *V* которого соответствуют элементам КСПД, а ребра *E* — физическим соединениям элементов КСПД. Сложность поиска элементов заключается в том, что простой обход графа КСПД может выдавать среди множества элементов те, которые не задействованы в реальных сетях в рассматриваемом ИП (см рисунок 1).

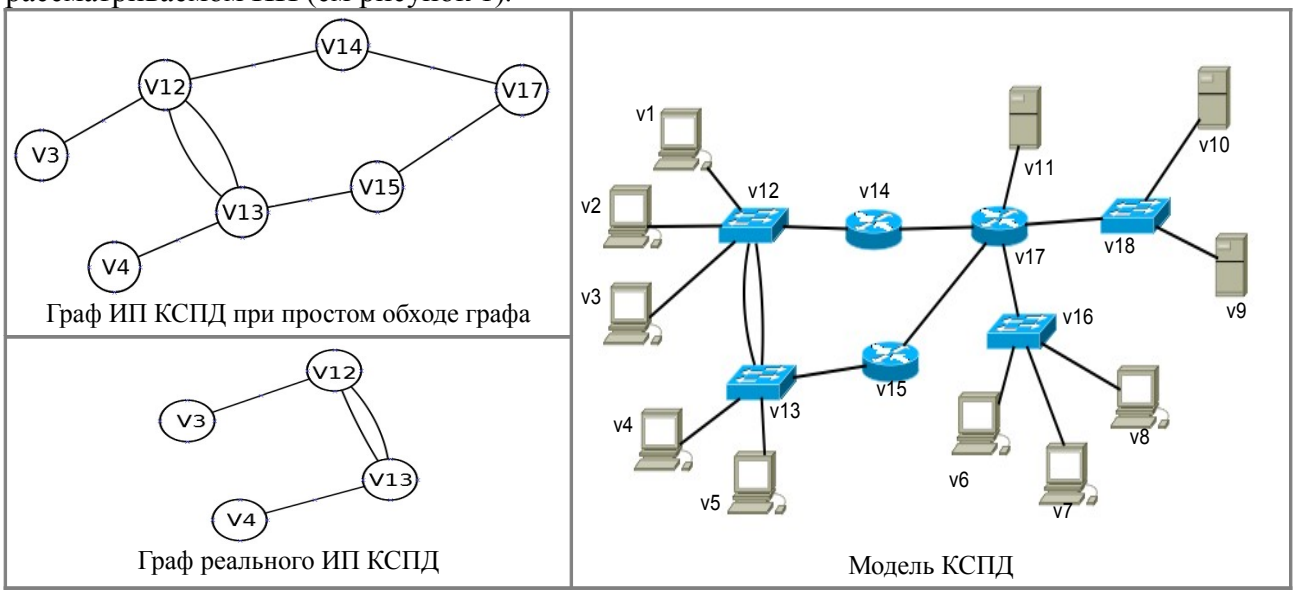

Рисунок 1 — Проблема выявления элементов ИП КСПД

Цель работы. Целью данной работы является разработка методики автоматизированного определения множества элементов корпоративной сети передачи данных (далее КСПД), задействованных в реализации заданного информационного процесса. Для достижения цели поставлены и решены следующие задачи:

1) анализ многоуровневого подхода построения КСПД;
2) разработка правил построение КСПД на некоторых уровнях модели *ISO OSI*. Ввод основных обозначение. Математическое описание;
3) разработка алгоритмов поиска всех элементов КСПД заданного информационного процесса (далее ИП);
4) тестовый расчет.

Объектом исследования является корпоративная сеть передачи данных.

Предметом исследования является методика автоматизированного определения множества элементов КСПД, задействованных в реализации заданного ИП.

Многоуровневая модель. Для выявления элементов КСПД задействованных в ИП используется многоуровневый подход построения КСПД, разработанной на кафедре ИЗИ. Основой подхода является построение графов, отображающих КСПД на нескольких уровнях эталонной модели *ISO OSI*, представленное в [2], [3]. Общая схема многоуровневой модели представлена на рисунке 2.

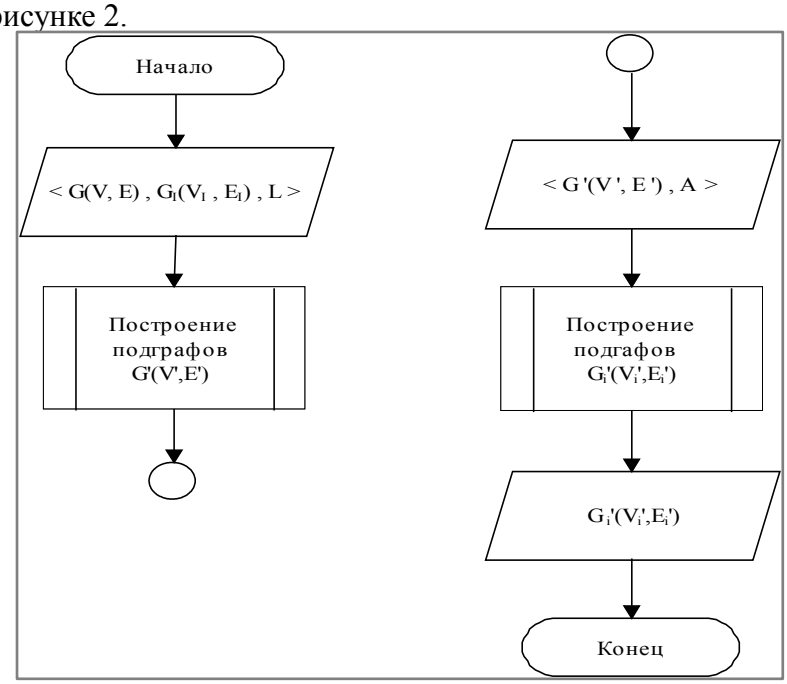

Рисунок 2 — Общая схема многоуровневой модели

В разработанной методике вводятся следующие обозначения:

1) *G(V, E)* — граф КСПД;
2) $G_I(V_I, E_I)$ — граф всех ИП КСПД;
3) G'(V', E') — отображение КСПД на физическом уровне;
4) *G''(V'', E'')* — отображение КСПД на канальном уровне;
5) *G''' (V''', E''')* — отображение КСПД на сетевом уровне;
6) *G''''(V'''', E'''')* — отображение КСПД на прикладном уровне;
7) *I* — множество всех ИП КСПД;
8) i_C — рассматриваемый ИП;
9) $G_i(V_i, E_i)$ — граф ИП КСПД;
10) $G'_i(V'_i, E'_i)$ — отображение графа ИП КСПД на физическом уровне;
11) $G''_i(V''_i, E''_i)$ — отображение графа ИП КСПД на канальном уровне;
12) $G'''_i(V'''_i, E'''_i)$ — отображение графа ИП КСПД на сетевом уровне;
13) $G''''_i(V''''_i, E''''_i)$ — отображение графа ИП КСПД на прикладном уровне;
14) *P* — множество оконечных узлов;
15) *R* — множество маршрутизаторов;
16) *Sw* — множество коммутаторов;
17) *H* – множество концентраторов;
18) *O* — множество оставшихся узлов;
19) *A* – множество весов ребер графа $G'''i(V'''_i, E'''_i)$.

В качестве входных параметров выступают граф КСПД *G*, граф всех ИП КСПД G_I и множество весов ребер графа КСПД сетевого уровня *A*. Методика предполагает выполнения 2-х этапов: отображения графа КСПД на рассматриваемых уровнях модели *ISO OSI* снизу вверх, и отображение графа заданного ИП КСПД на тех же уровнях сверху вниз.

Построение графом КСПД снизу вверх. В рамках первого этапа были разработаны

правила выбора вершин и ребер графа подлежащих удалению (уникальные для каждого уровня), а также следующие правила удаления вершин и ребер для построения графа КСПД на последующем уровне *ISO OSI*:

- удаление вершины сопровождается удалением всех инцидентных ей рёбер;
- вершина, не имеющая инцидентных рёбер, удаляется;
- удаление ребра, связывающего оконечное устройство с промежуточным, вызывает создание ребра между оконечным узлом и промежуточным устройством, связанным с оконечным, через удаленное инцидентное ребро.

На рисунке 3 представлены граф КСПД и граф всех ИП КСПД.

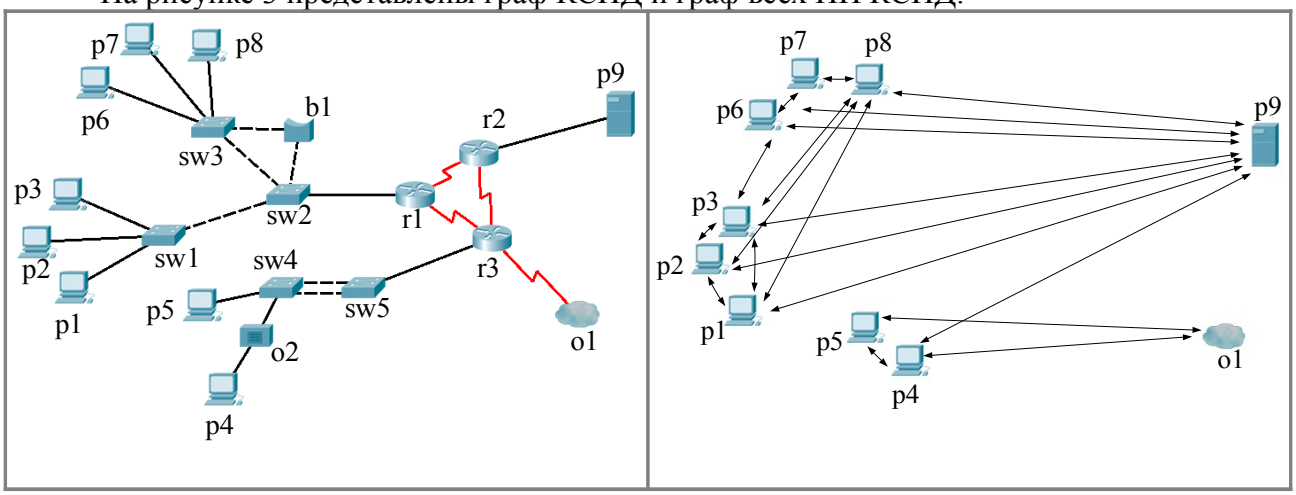

Рисунок 3 — Граф КСПД (слева) и граф всех ИП КСПД (справа)

По данным параметрам происходит построение графов КСПД на физическом, канальном, сетевом и прикладном уровнях (см рисунок 4).

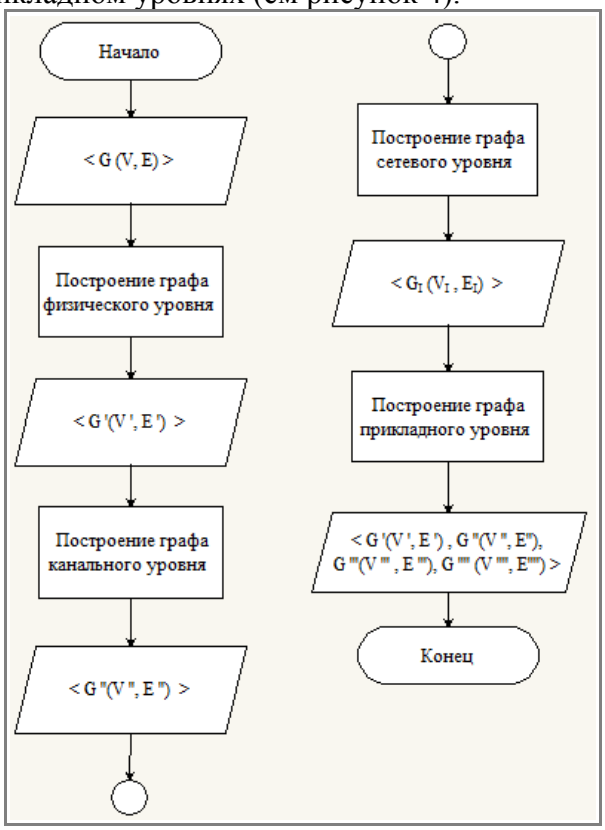

Рисунок 4 — Алгоритм построения графа КСПД на 4-х уровнях модели *ISO OSI*

Отображение КСПД на физическом уровне представлено на рисунке 5. На данном уровне КСПД присуща избыточность соединений.

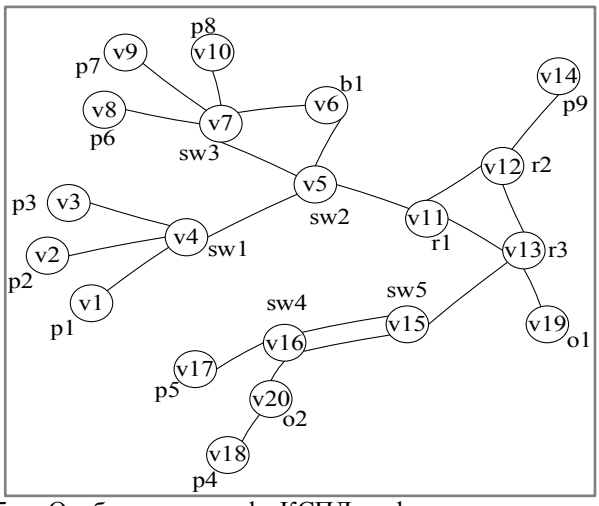

Рисунок 5 — Отображение графа КСПД на физическом уровне

На рисунке 6 показан процесс построения по графу КСПД физического уровня графа КСПД канального уровня. Предполагается, что на канальном уровне работает протокол *STP*, осуществляющий устранение избыточности связей.

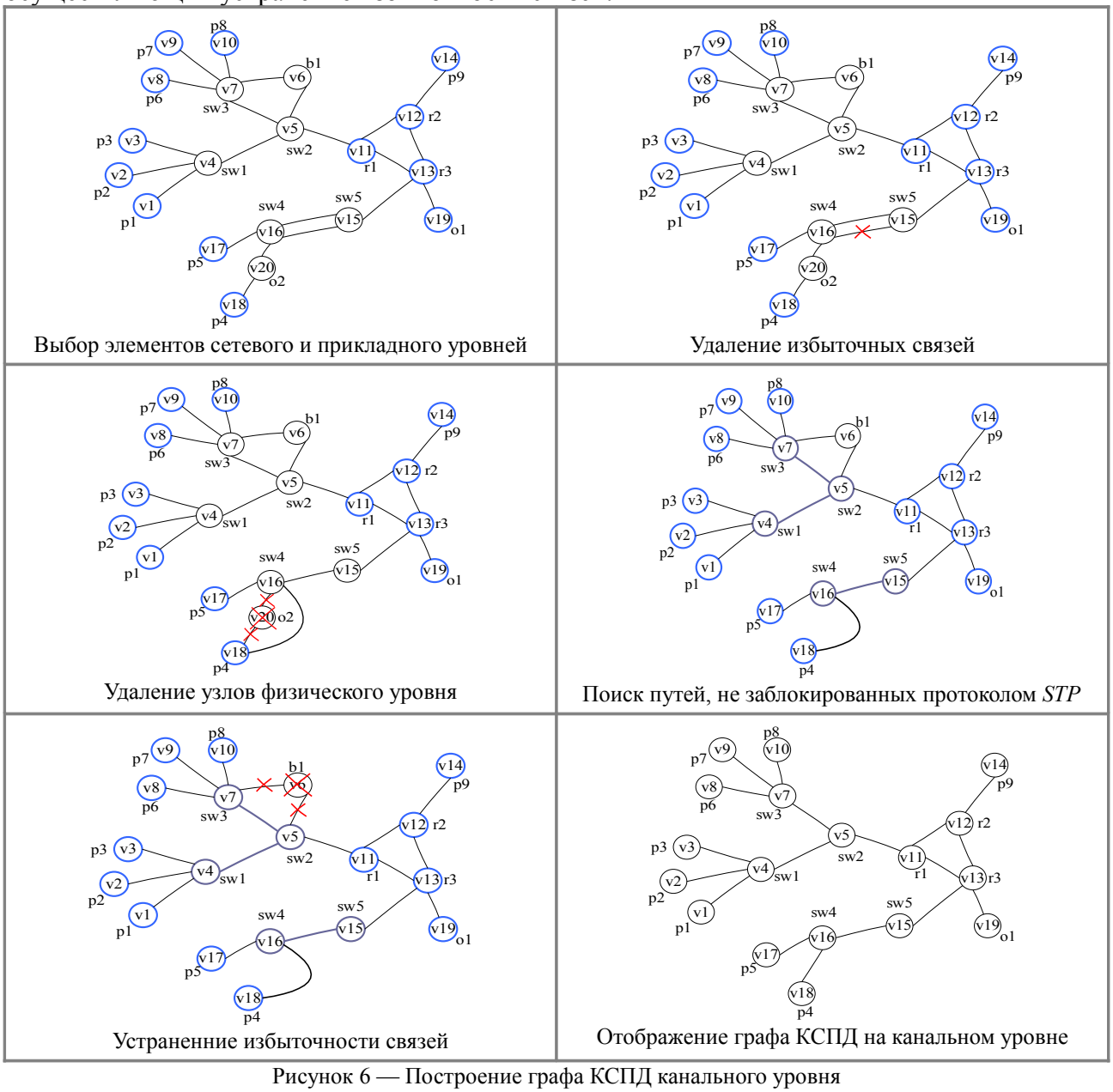

Рисунок 6 — Построение графа КСПД канального уровня

На рисунке 7 представлен процесс построения графа КСПД сетевого уровня. На сетевом уровне вводятся веса рёбер, необходимые на следующем этапе.

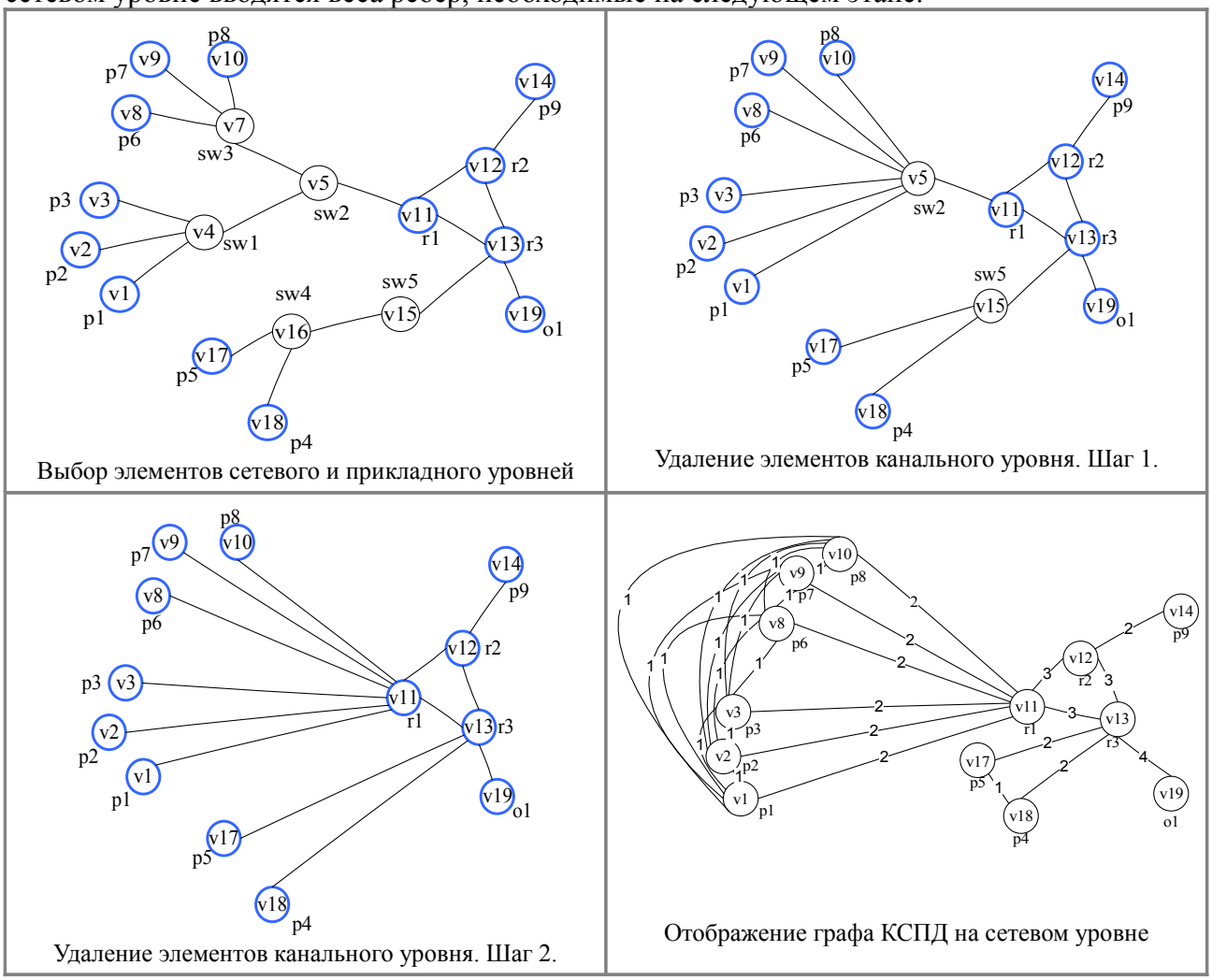

Рисунок 7 — Построение графа КСПД на сетевом уровне

На рисунке 8 показано отображение графа КСПД на прикладном уровне.

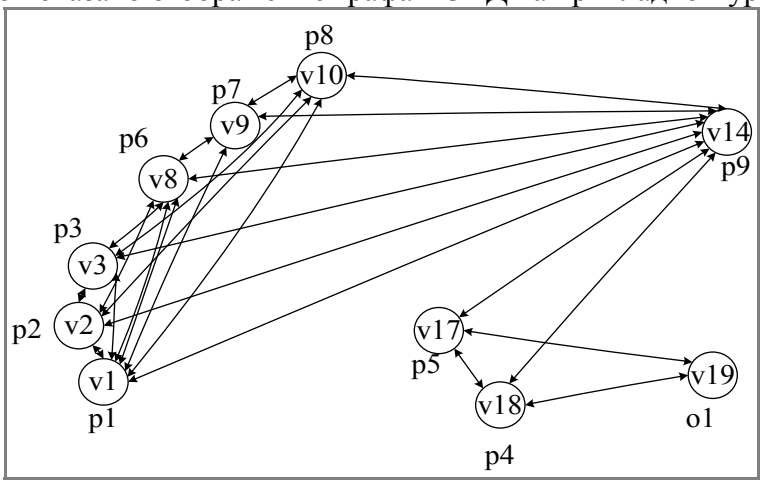

Рисунок 8 — Отображение графа КСПД на прикладном уровне

Построение графов ИП КСПД сверху вниз. В рамках второго этапа был разработаны алгоритм построения графов ИП КСПД для 4-х уровней модели *ISO OSI*:

− выделяются на граф КСПД заданного уровня накладывается граф ИП КСПД более верхнего уровня. В результате отмечаются элементы, между которыми необходимо «восстановить» связи;

− для восстановления связей используется алгоритм полного перебора графа КСПД заданного уровня. В результате получается граф ИП КСПД являющийся подграфом КСПД заданного уровня модели *ISO OSI*.

По полученным графам на предыдущем этапе и заданному ИП строится последовательность графов ИП КСПД на 4-х уровнях модели *ISO OSI* (см рисунок 9).

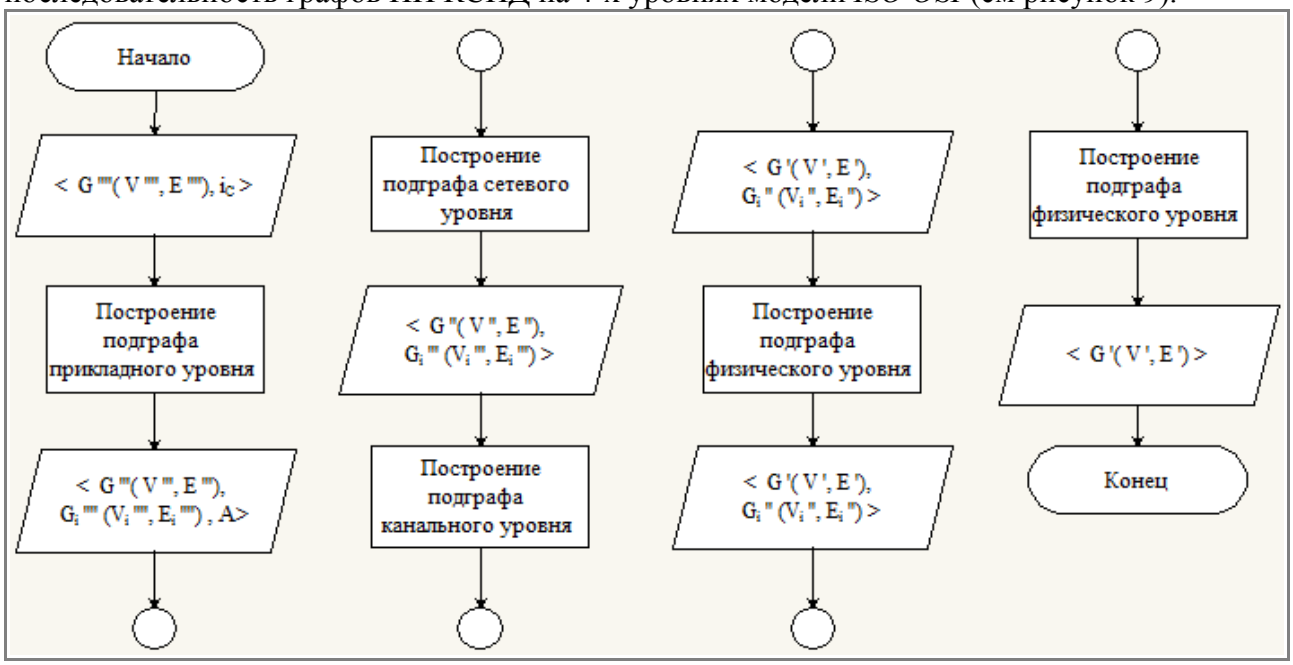

Рисунок 9 — Алгоритм построения графа ИП КСПД на 4-х уровнях модели *ISO OSI*

На рисунках 10 и 11 представлены отображения графа ИП КСПД на прикладном и сетевом уровнях соответственно. Для определения релевантных путей на сетевом уровне используются следующие правила:

− взаимодействие между двумя элементами сети отражается маршрутом с наименьшим весом;

− в маршруте не могут одновременно присутствовать ребра с весом 1 и ребра с другими весами. Иначе говоря, оконечные устройства не могут взаимодействовать с другими устройствами в сети через иные оконечные устройства.

На рисунке 12 и 13 представлены отображения графов ИП КСПД на канальном и физическом уровне соответственно. Итоговый граф ИП КСПД представлен на рисунке 14.

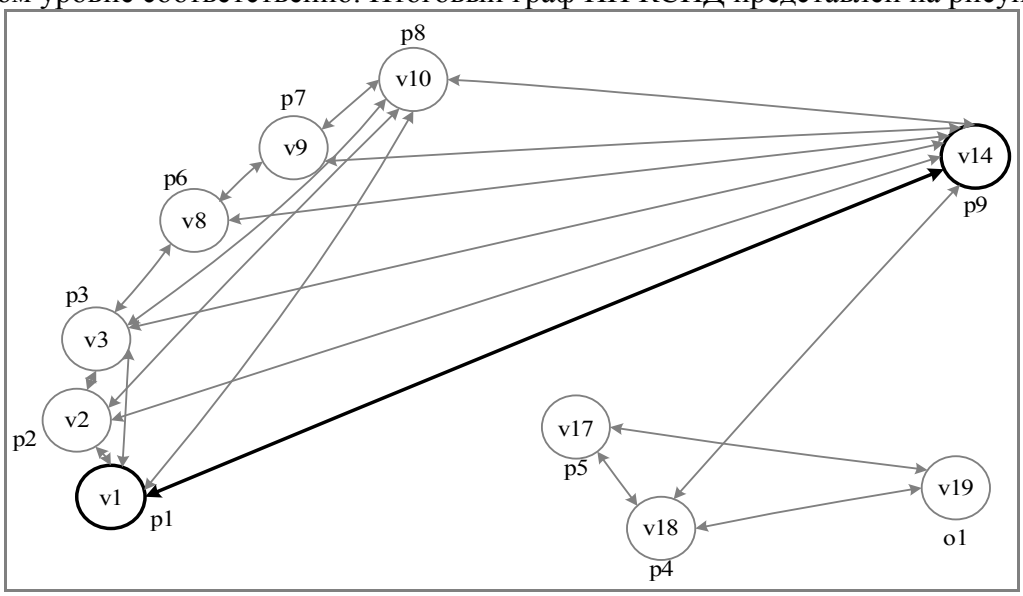

Рисунок 10 — Отображение графа ИП КСПД на прикладном уровне

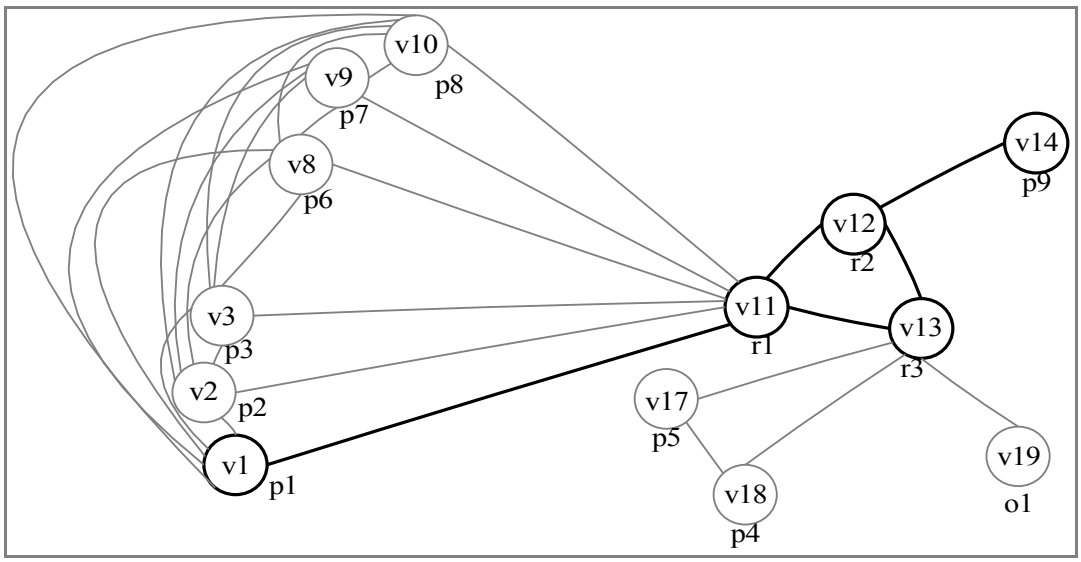

Рисунок 11 — Отображение графа ИП КСПД на сетевом уровне

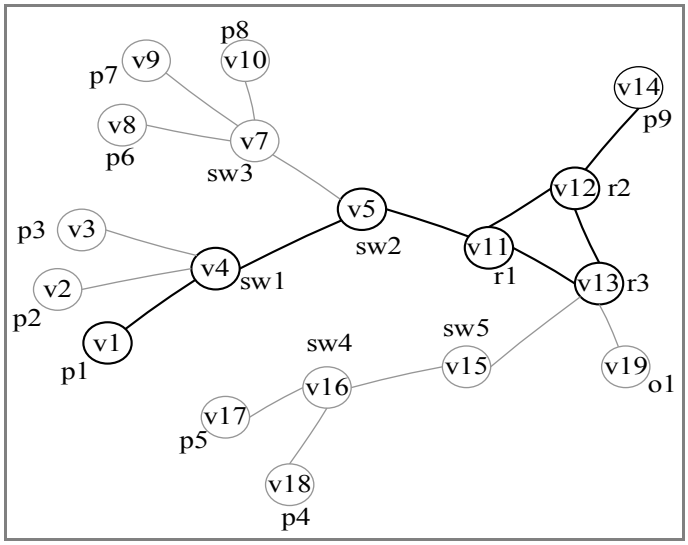

Рисунок 12 — Отображение графа ИП КСПД на канальном уровне

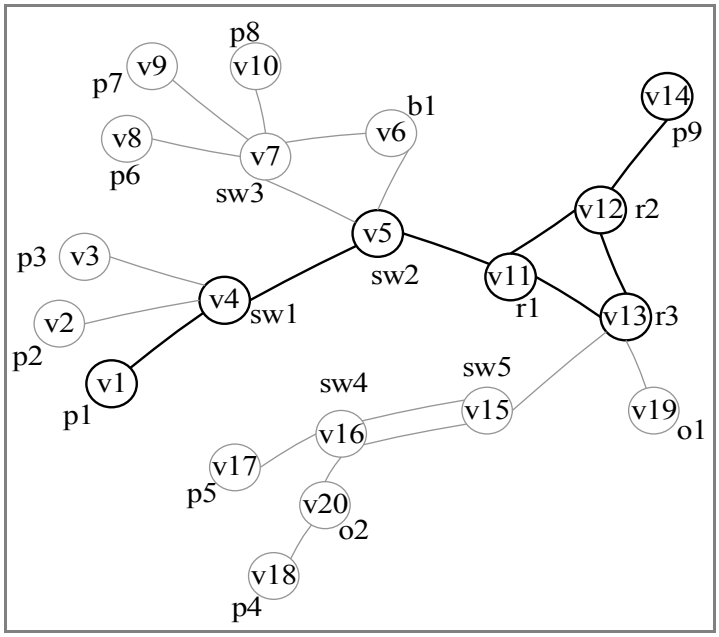

Рисунок 13 — Отображение графа ИП КСПД на физическом уровне

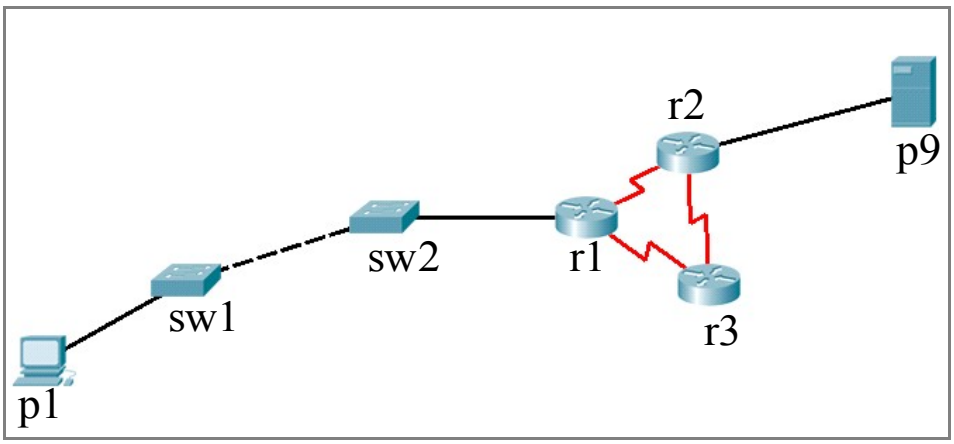

Рисунок 14 — Граф ИП КСПД

Выводы. В рамках выполнения данной работы был проведен анализ графовой модели сети передачи данных и многоуровневого подхода построения КСПД.

Была разработана методика автоматизированного выявления элементов КСПД для рассматриваемого ИП. Методика включает:

- перечень входных и выходных параметров;
- алгоритм многоуровневого представления КСПД (построение графов КСПД снизу вверх на рассматриваемых уровнях *ISO OSI*);
- алгоритм многоуровневого представления ИП КСПД (построение графов ИП КСПД сверху вниз на рассматриваемых уровнях *ISO OSI*);
- правила выбора и удаления вершин и ребер графа КСПД при переходе на следующий уровень (снизу вверх);
- правила выбора и добавления вершин и ребер графа ИП КСПД при переходе на следующий уровень (сверху вниз).

Был произведен тестовый расчет.

Список литературы: **1.** И.Ю. БОГОМАЗОВА, Д.В. МИШИН, М.Ю. МОНАХОВ ГРАФОВЫЕ МОДЕЛИ ПРЕДСТАВЛЕНИЯ СЕТЕЙ ПЕРЕДАЧИ ДАННЫХ // Материалы НТС кафедры "Информатика и защита информации", - 2012. [Электронный ресурс]. URL:http://izi.vlsu.ru/HTC/17.pdf. **2.** И.Ю. Богомазова, М.Ю. Монахов, М.М. Монахова, Д.В. Мишин «Графовая модель сети передачи данных» [Электронный ресурс].URL: http://izi.vlsu.ru/HTC/31.pdf. **3.** И.Ю. Богомазова, М.Ю. Монахов, М.М. Монахова, Д.В. Мишин «Графовая модель сети передачи данных. Обобщение результатов.» [Электронный ресурс]. URL: http://izi.vlsu.ru/HTC/39.pdf.