И.Ю. БОГОМАЗОВА, студентка гр. КЗИ-108;
М.Ю. МОНАХОВ, д.т.н., профессор;
М.М. МОНАХОВА, ассистент;
Д.В. МИШИН, ст. преподаватель.

ГРАФОВАЯ МОДЕЛЬ СЕТИ ПЕРЕДАЧИ ДАННЫХ. ОБОБЩЕНИЕ РЕЗУЛЬТАТОВ

Рассмотрены основные результаты работы и дано их краткое описание. Приведен наглядный пример применения созданной уровневой графовой модели сети передачи данных.

Ключевые слова: СЕТЬ ПЕРЕДАЧИ ДАННЫХ, ГРАФОВАЯ МОДЕЛЬ, УРОВЕНЬ, ЭЛЕМЕНТ, СВЯЗЬ, ГРАФ, ВЕРШИНА, РЕБРО, БИЗНЕС-ПРОЦЕСС, ИНФОРМАЦИОННЫЙ ПРОЦЕСС.
11 рис., 0 табл., 2 источника.

Целью данной работы является создание графового представления сети передачи данных (СПД), позволяющего моделировать сетевые атаки.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ предметной области;
2. Исследовать и адаптировать к поставленным задачам понятийный аппарат данной предметной области;
3. Выбрать подход к рассмотрению СПД;
4. Разработать и формализовать графовые модели СПД;
5. Проиллюстрировать данный подход к моделированию СПД на исходной СПД.

В результате анализа предметной области был описан объект моделирования – СПД. Под СПД понимаем организованную совокупность локализованных технических и программных средств реализации функций СПД. Под элементами СПД понимаем оконечные устройства, коммуникационное оборудование и коммуникационные каналы связи.

Кроме того были выделены основные методы моделирования систем [1], особое внимание уделено графовым моделям. При анализе опыта применения графовых моделей для представления СПД выяснено, что наиболее употребительным является классический подход к представлению сетей графами.

Так же рассмотрены уровневые подходы к представлению СПД: сетевые модели ISO OSI и TCP/IP, - приведены примеры сетевых атак, статистика по атакам, проведен обзор работ по моделированию атак.

Анализ существующих моделей СПД [1] позволил сделать вывод о том, что в задачах моделирования сетевых атак в условиях многообразия и сложности структур СПД современных предприятий, решение применения графовых моделей, а именно, адаптированного классического графового представления СПД в виде графа G, вершины которого V сопоставляются с узлами сети, а ребра E соответствуют линиям связи между узлами, является наилучшим.

Авторами предлагается внедрение многоуровневого подхода в построение графовой модели СПД [2]. В основу иерархии положена модель ISO OSI. К рассмотрению принимаются уровни модели ISO OSI, на которых проводятся самые распространенные атаки, то есть физический, канальный, сетевой и прикладной уровни.

Проиллюстрируем применеие созданной модели на примере исходной сети из 27 устройств, изображенной на рисунке 1.

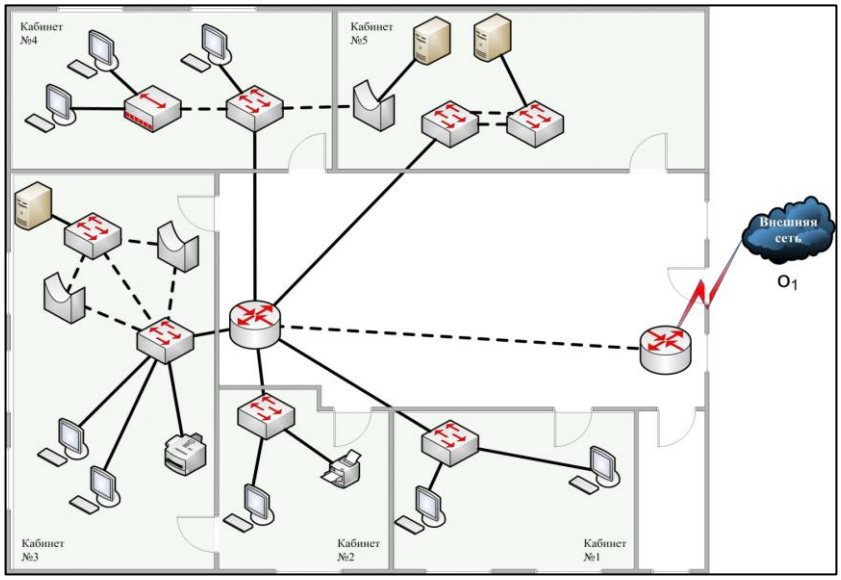

Рисунок 1 – Исследуемая СПД

Основные множества элементов данной СПД (рисунок 2):

1. Оконечные устройства: $P = \{p_1, p_2, \ldots, p_{20}\}$.

2. Концентраторы: $H = \{h_1\}$.

3. Мосты: $B = \{b_1, b_2, b_3\}$.

4. Коммутаторы: $S = \{s_1, s_2, .., s_7\}$.

5. Маршрутизаторы: $R = \{r_1, r_2, .., r_8\}$.

6. Другие устройства: $O = \{o_1\}$. В данном случае o_1 – внешняя сеть, представляет собой некоторую виртуальную совокупность взаимосвязанных сетевых устройств, расположенных за пределами СПД организации.

Количество элементов в данной СПД без коммуникационных линий связи $n = |P| + |H| + |B| + |S| + |R| = 26$, и один внешний элемент.

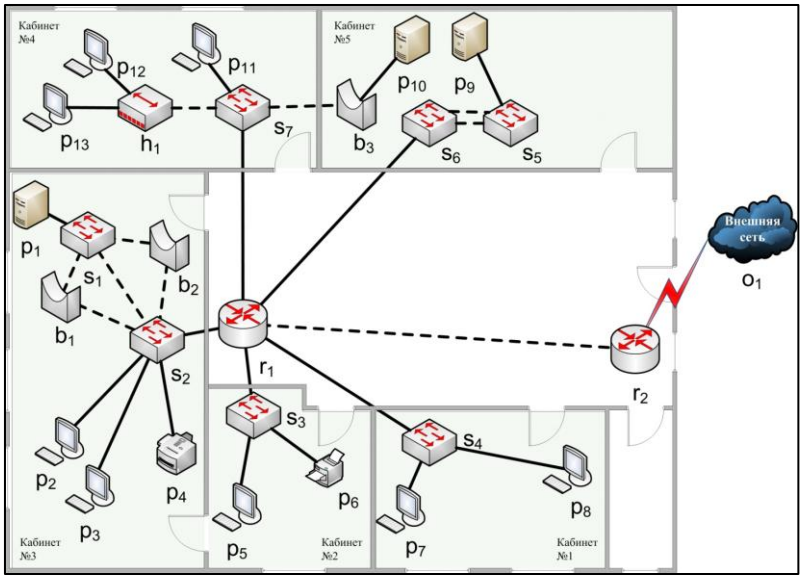

Рисунок 2 – Расстановка обозначений элементов исследуемой СПД

На физическом уровне СПД может быть представлена неориентированным мультиграфом $G' = (V', E')$ (рисунок 3) в силу возможной избыточности соединений. На физическом уровне работают все сетевые устройства и им соответствуют вершины графа $V' = \{v_1, v_2, .., v_{27}\} = P \cup R \cup S \cup H \cup B \cup O$. E' - мультимножество ребер, соответствующих непосредственным физическим соединениям между устройствами с помощью линий связи.

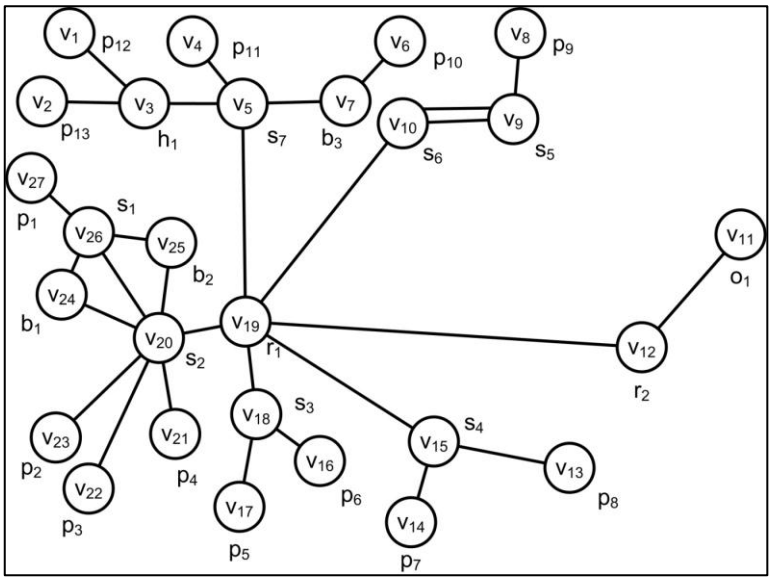

Рисунок 3 – Физический уровень модели исследуемой СПД

Сеть на канальном уровне представим в виде неориентированного графа без петель $G'' = (V'', E'')$ (рисунок 4). На графе сети передачи данных должны быть отражены только элементы $V'' = \{v_1, v_2, .. , v_{27}\} \backslash \{v_{24}, v_{25}\}$, участвующие в передаче потоков данных (взаимодействии по сети). Это связано с тем, что на канальном уровне работают протоколы, устраняющие избыточность в сети с коммутаторами (мостами). $V'' = P \cup R \cup S' \cup H \cup B' \cup O'$, $S' = S$, $B' = \{b_3\}, O' = O$. E'' - множество ребер, соответствующих непосредственным физическим соединениям между устройствами с помощью линий связи, по которым осуществляется передача информации (незаблокированным).

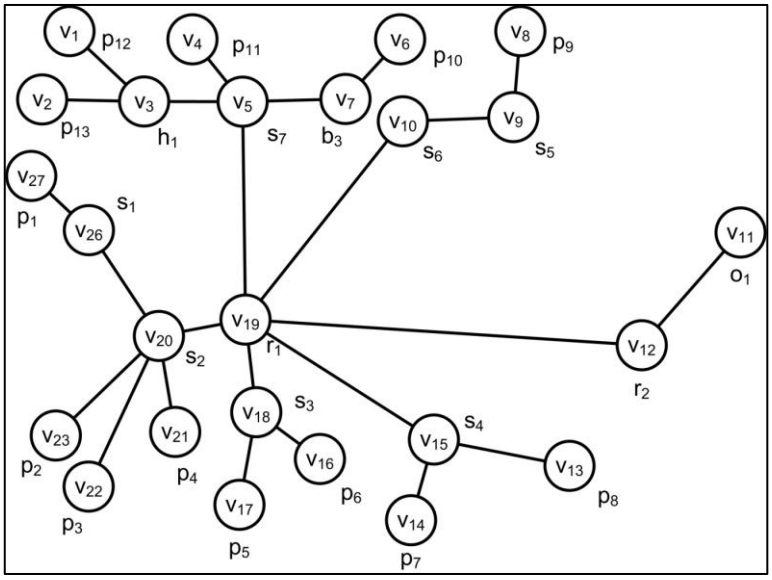

Рисунок 4 – Канальный уровень модели исследуемой СПД

На третьем уровне (сетевом) представим сеть в виде неориентированного взвешенного графа без петель $G''' = (V''', E''')$ (рисунок 5). V''' –вершины, соответствующие элементам СПД, работающим на сетевом уровне. $V''' = \{v_1, v_2, .. , v_{27}\} \backslash \{v_3, v_5, v_7, v_9, v_{10}, v_{15}, v_{18}, v_{20}, v_{24}, v_{25}, v_{26}\}$, $V''' = P \cup R \cup S'' \cup O''$; $S'' = O, O'' = O$. E''' – множество ребер, соответствующих непосредственным или через устройства более низкого уровня (канального) связям между устройствами.

Каждое ребро $e''' \in E'''$ снабжено положительным весом, причем ребрам, соединяющим оконечные устройства между собой в пределах каждого широковещательного домена, присваивается минимальный вес a=1, ребра, соединяющие оконечные устройства с маршрутизатором в пределах каждого широковещательного домена, должны иметь вес b=2, а ребра, связывающие маршрутизаторы, получают динамически меняющийся вес, исходя из совокупной оценки метрик.

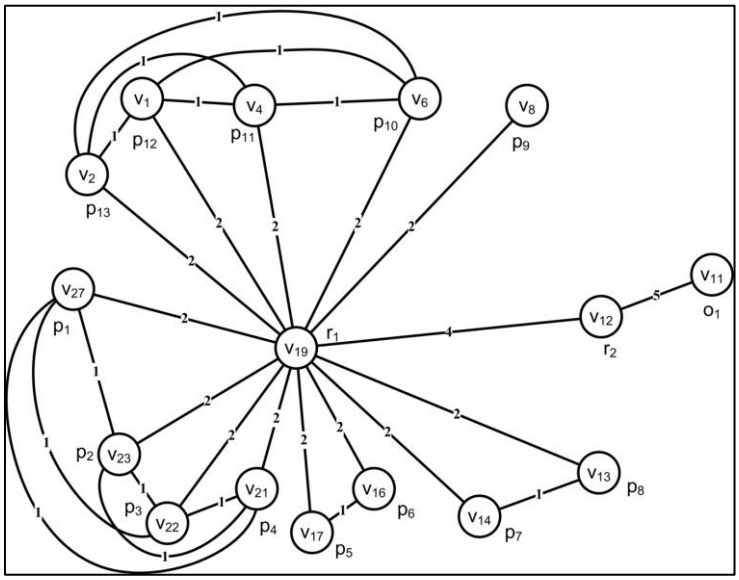

Рисунок 5 – Сетевой уровень модели исследуемой СПД

СПД на прикладном уровне представим в виде ориентированного мультиграфа без петель $G'''' = (V'''', E'''')$ (рисунок 6). Вершины V'''' соответствуют оконечным устройствам, на которых работают приложения, взаимодействующие по сети.

$V'''' = \{v_1, v_2, v_4, v_6, v_8, v_{11}, v_{13}, v_{14}, v_{16}, v_{17}, v_{21}, v_{22}, v_{23}, v_{27}\}$.

E'''' – множество дуг, соответствующих связям по передаче некоторой информации (в том числе служебной) между приложениями на устройствах.

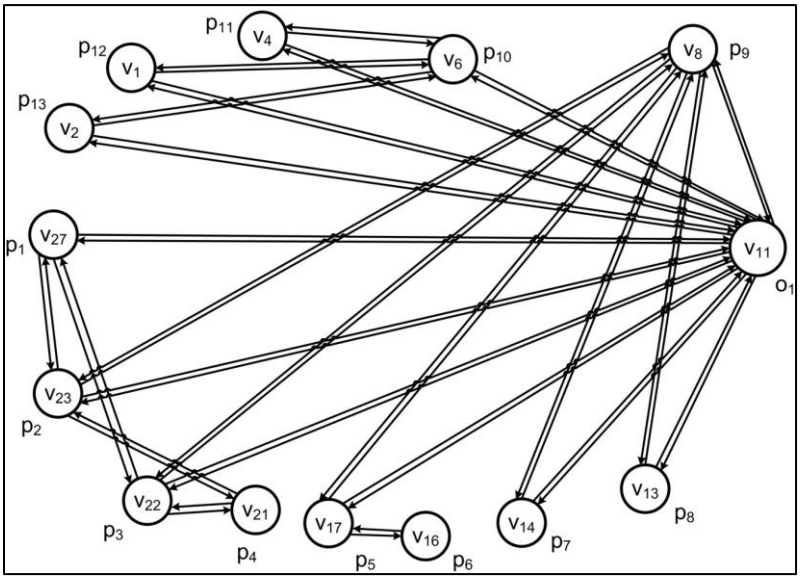

Рисунок 6 – Прикладной уровень модели исследуемой СПД

На прикладном уровне могут быть показаны бизнес-процессы (БП). К примеру, БП1 (например, работа с корпоративной почтой) представлен графом G_1'''' - подграфом графа G'''' - на рисунке 7.

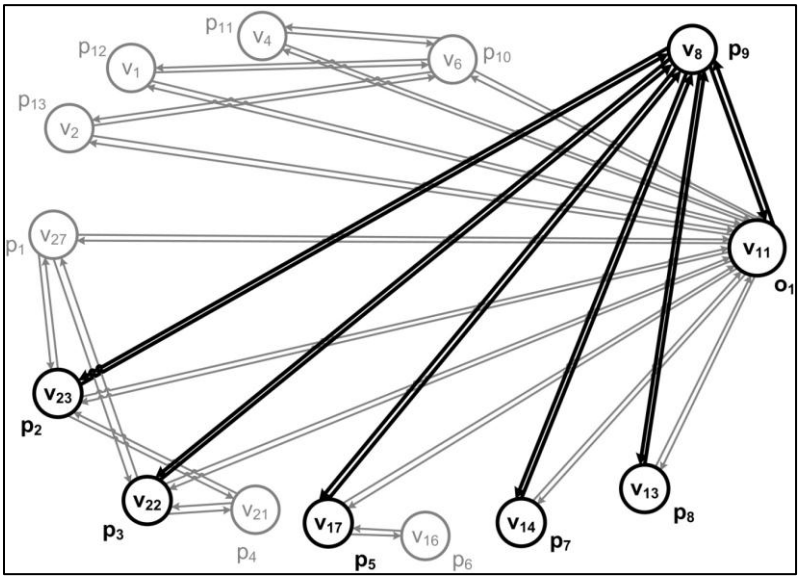

Рисунок 7 – Бизнес-процесс 1 на графе СПД прикладного уровня

В рамках бизнес-процессов выделяют информационные процессы (ИП). ИП1 (v_1 - v_{23}) в рамках БП1 представлен графом G_{11}'''' (рисунок 8) - подграфом графа G_1'''' и соответственно подграфом G''''.

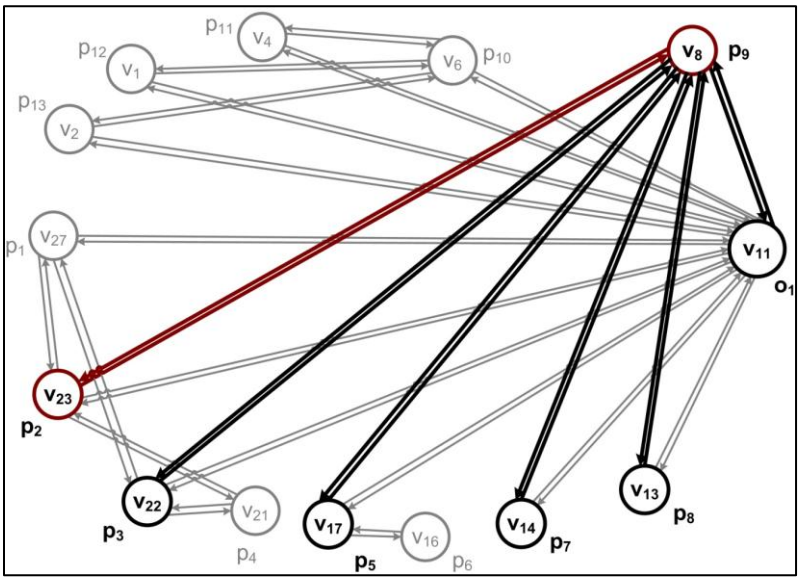

Рисунок 8 – Выделение ИП1 в рамках бизнес-процесса 1

Выделенные информационные процессы могут быть представлены и на других уровнях модели. Рассмотрим ИП1.

ИП1 на сетевом уровне представлен графом G_{11}''' (рисунок 9) - подграфом графа G'''.

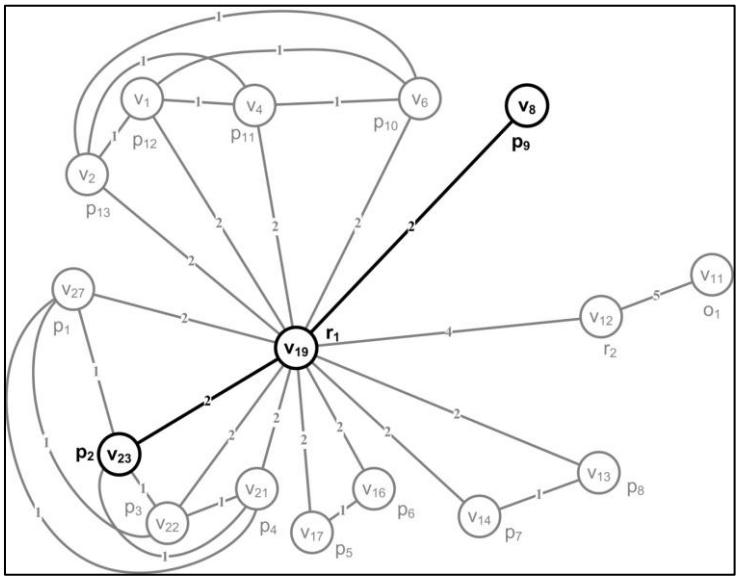

Рисунок 9 – Представление ИП1 на сетевом уровне

ИП1 на канальном уровне представлен графом G_{11}'' (рисунок 10) - подграфом графа G''.

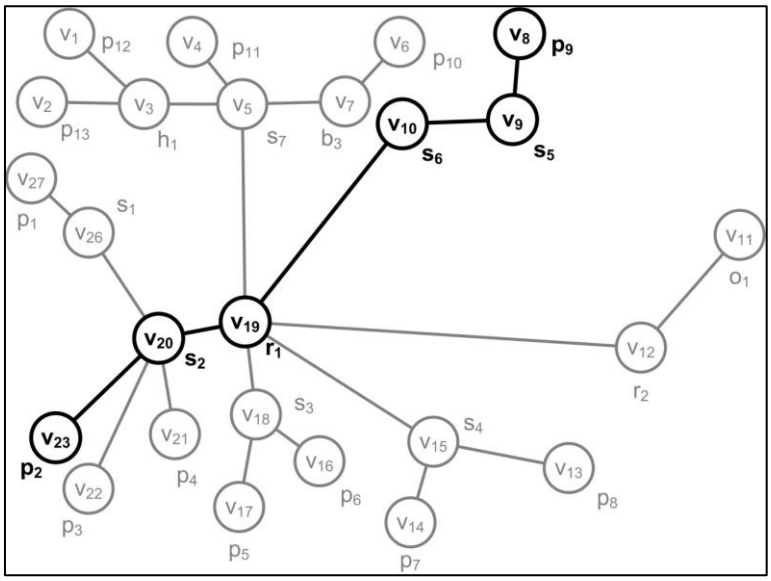

Рисунок 10 – Представление ИП1 на канальном уровне

ИП1 на физическом уровне представлен графом G_{11}' (рисунок 11) - подграфом графа G'.

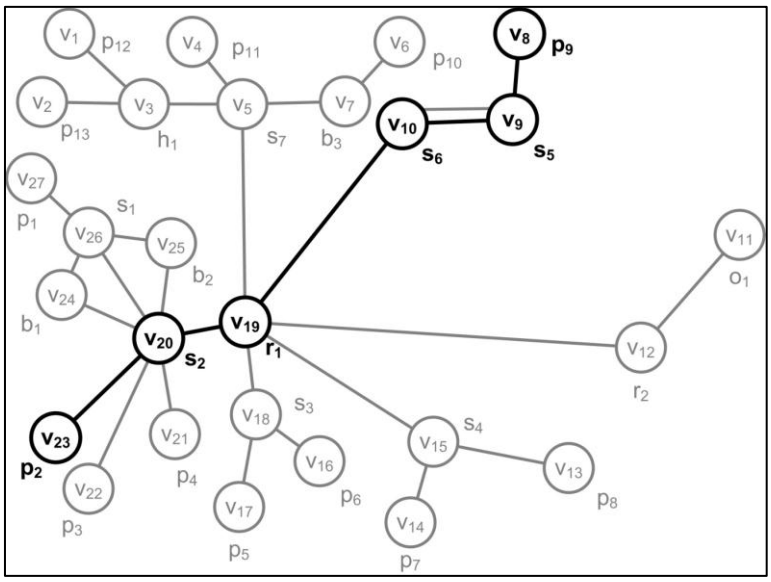

Рисунок 11 – Представление ИП1 на физическом уровне

На этапе разработки были получены следующие результаты:

1. Разработаны графовые представления СПД на каждом из выделенных уровней.

2. Разработана методика моделирования СПД.

3. Описано взаимодействие между элементами СПД и ограничения: взаимодействие показывается путем на графе. Под путем (маршрутом) по графу, соединяющим две вершины u и v, понимаем простую цепь, то есть все вершины, а следовательно, и все ребра в данном маршруте различны.

4. Разработаны принципы согласования между уровнями и правила удаления элементов.

5. Выделены основные характеристики элементов графовой модели СПД (присущие ИР, уязвимости, типы нарушителей, защитные механизмы).

Подведем итоги проделанной работы:

1. Описан объект моделирования, даны основные понятия предметной области. Обобщен анализ опыта применения графовых моделей для представления СПД и моделирования сетевых атак. Принято решение взять за основу моделирования классическую графовую модель. Предложен уровневый подход к рассмотрению СПД на основе модели ISO OSI.

2. Разработано уровневое графовое представление СПД. Описана методика создания модели СПД. Определены правила взаимодействия между элементами СПД. Разработаны правила согласования между уровнями. Выделены основные характеристики элементов графовой модели СПД.

3. Проиллюстрирована возможность применения разработанной модели СПД.

Описанное представление СПД применимо для моделирования сетевых атак, также может использоваться в решении задачи анализа защищенности информационной системы, при расстановке приоритетов функциональных элементов корпоративной СПД.

Литература

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 // Материалы НТС кафедры "Информатика и защита информации", - 2012. [Электронный ресурс]. URL:http://izi.vlsu.ru/HTC/31.pdf