

УДК 004.021

**О ПРИМЕНЕНИИ УРОВНЕВОЙ МОДЕЛИ  
КОРПОРАТИВНОЙ СЕТИ В ЗАДАЧАХ ОБЕСПЕЧЕНИЯ  
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
ПРЕДПРИЯТИЯ ТЕКСТИЛЬНОЙ ПРОМЫШЛЕННОСТИ**

**ON THE APPLICATION TIER MODEL  
OF CORPORATE NETWORKS IN PROBLEMS  
OF INFORMATION SECURITY OF THE ENTERPRISES  
OF THE TEXTILE INDUSTRY**

*Д.В. МИШИН, И.Ю. МИШИНА*  
*D.V. MISHIN, I.YU. MISHINA*

(Владимирский государственный университет  
имени Александра Григорьевича и Николая Григорьевича Столетовых)  
(Vladimir State University named after Alexander and Nikolai Stoletovs)  
E-mail: mishin.izi@gmail.com

*В статье предлагается уровневая графовая модель корпоративной сети  
предприятия текстильной промышленности, позволяющая при построе-*

*нии системы защиты информации определить принадлежности компонент сети подсистемам АИС.*

*The article proposes a level graph model of the corporate network of the textile industry, allowing the construction of information security system to determine the belonging of the network component of the AIS subsystems.*

**Ключевые слова:** уровневая графовая модель, система защиты информации, конфиденциальная информация, подсистема АИС.

**Keywords:** layered graph model, the system of information protection of confidential information, the subsystem AIS.

В настоящее время на большинстве предприятий текстильной промышленности (ПТП) исследуемого региона (Ивановской области) осуществляется автоматизированная обработка конфиденциальной информации (КИ), а значит – для ПТП актуальна задача обеспечения безопасности КИ. Как правило, ПТП обрабатывают следующие виды КИ: коммерческую тайну, персональные данные (ПДн), информацию о криптографических ключах и среде функционирования средств криптографической защиты информации (СКЗИ) или иную КИ. Требования к защите КИ, в зависимости от ее вида, может устанавливать собственник (в случае коммерческой тайны), или защита должна осуществляться в соответствии с Федеральным законодательством (например, для ПДн) и нормативно-правовыми актами регуляторов (ФСБ, ФСТЭК). Очевидно, что количество реализуемых защитных мер, типы и виды технических средств защиты, необходимая квалификация специалистов, а следовательно, и стоимость системы защиты информации (СЗИ) для различных видов КИ будет различной. Анализ автоматизированных информационных систем (АИС) ПТП Ивановской области позволил выявить следующие принципиальные для проектирования СЗИ особенности: территориально распределенная структура; сегменты объединяются через общедоступные сети; используются различные аппаратно-программные платформы; для повышения производительности и надежности реализована избыточность каналов связи, сетевого и серверного оборудования; под-

системы АИС, обрабатывающие КИ различных видов, функционируют на единой информационно-технической инфраструктуре – корпоративной сети ПТП (КСПТП). В данной ситуации принадлежность компонент КСПТП (отдельных средств вычислительной техники, сетевого и периферийного оборудования) к различным подсистемам АИС ПТП (обрабатывающим КИ заданного вида) неочевидна, что влечет ошибки при проектировании и, как следствие, значительные дополнительные расходы на реализацию СЗИ ПТП. Авторы считают, что одной из актуальных является задача автоматизации определения подмножества компонент КСПТП, обеспечивающих функционирование каждой из подсистем АИС ПТП.

Анализ технологических и бизнес-процессов ПТП, как правило, позволяет выявить множество подсистем АИС ПТП, клиентские и серверные компоненты каждой из выявленных АИС, построить граф КСПТП [1]. Для выявления промежуточных (сетевых компонент) и построения подграфов подсистем АИС ПТП требуются дополнительные конструкции, так как построенные при помощи традиционных алгоритмов обхода графа, подграфы подсистем АИС ПТП могут оказаться неполными или содержать пути, не соответствующие логике сетевых протоколов [2], [3]. Авторами разработана уровневая графовая модель КСПТП и методика ее применения, которые могут помочь в разрешении возникшей ситуации. По модели КСПТП представляется графами на четырех уровнях

ISO OSI: физическом (L1), канальном (L2), сетевом (L3) и прикладном (L7).

Определим основные множества элементов КСПТП:

множество конечных устройств

$$P = \{p_1, p_2, \dots, p_f \mid f \in \mathbb{N}\},$$

множество концентраторов

$$H = \{h_1, h_2, \dots, h_g \mid g \in \mathbb{N}\},$$

множество мостов

$$B = \{b_1, b_2, \dots, b_i \mid i \in \mathbb{N}\},$$

множество коммутаторов

$$S = \{s_1, s_2, \dots, s_j \mid j \in \mathbb{N}\},$$

множество маршрутизаторов

$$R = \{r_1, r_2, \dots, r_k \mid k \in \mathbb{N}\},$$

множество

$$O = \{o_1, o_2, \dots, o_m \mid m \in \mathbb{N}\}$$

других устройств в рассматриваемой КСПТП. Количество элементов в КСПТП без коммуникационных линий связи

$$n = |P| + |H| + |B| + |S| + |R|.$$

На L1 необходимо отобразить все элементы КСПТП, в том числе линии связи. Поскольку КСПТП может характеризоваться некоторой избыточностью оборудования и/или соединений, представим сеть на L1 в виде неориентированного мультиграфа без петель: упорядоченной пары:

$$G' = (V', E'),$$

где  $V' = V = \{v_1, v_2, \dots, v_n\}$  – множество вершин графа такое, что:

$$V = P \cup R \cup S \cup H \cup B \cup O, \\ n' = n = |P| + |R| + |S| + |H| + |B| + |O|;$$

$E'$  – мультимножество неупорядоченных пар вершин (семейство подмножеств множества:

$$V^{(2)} = \{(v_i, v_j) = (v_j, v_i) \mid v_i, v_j \in V, i \neq j\}$$

– ребер, соответствующих непосредственным физическим соединениям между устройствами с помощью линий связи.

На графе КСПТП L2 должны присутствовать только элементы, участвующие в сетевом взаимодействии. Это связано с тем, что в сетях с коммутаторами (мостами) на канальном уровне работают протоколы, блокирующие избыточные соединения (STP и его расширения). Таким образом, КСПТП на L2 представляется в виде неориентированного графа без петель:

упорядоченной пары

$$G'' = (V'', E''),$$

где  $V''$  – множество вершин графа такое, что:

$$V'' \subset V'$$

и

$$V'' \subset V,$$

$$V'' = P \cup R \cup S' \cup H \cup B' \cup O',$$

$$n'' = |P| + |R| + |S'| + |H| + |B'| + |O'|; S' \subset S$$

– множество коммутаторов, работающих на L2 в рассматриваемой сети;  $B' \subset B$  – множество мостов, работающих на L2 в рассматриваемой сети; также учитываются другие устройства, имеющиеся в рассматриваемой КСПТП и работающие на L2 уровне ( $O'$ ).  $E'' = (E'' \subset V''^{(2)})$  множество ребер, соответствующих незаблокированным непосредственным физическим соединениям между устройствами с помощью линий связи, по которым осуществляется передача информации.

На L3 изобразим КСПТП в виде неориентированного взвешенного графа без петель:

упорядоченной пары

$$G''' = (V''', E'''),$$

где  $V'''$  – множество вершин графа такое, что:

$$V''' \subset V''$$

и соответственно

$$V''' \subset V', V''' \subset V, V''' = P \cup R \cup S'' \cup O'', \\ n''' = |P| + |R| + |S''| + |O''|; S'' \subset S$$

– множество коммутаторов L3 в рассматриваемой сети; также могут быть учтены другие устройства, имеющиеся в рассматриваемой КСПТП и работающие на L3(O'').  
 $E'''$  – ( $E''' \subset V'''^{(2)}$ )

$e''' \in E'''$  снабжено весом  $\ell_{E'''}(e''') > 0$ , причем ребрам, соединяющим оконечные устройства между собой в пределах каждого широковещательного домена, присваивается минимальный вес  $a \in \mathbb{N}$ , ребра, соединяющие оконечные устройства с маршрутизатором в пределах каждого широковещательного домена, должны иметь вес:

$$b \in \mathbb{N} (b > 1/2 a),$$

а ребра, связывающие маршрутизаторы, получают динамически меняющийся вес  $\ell_{E'''}(e''')$ , исходя из совокупной оценки метрик.  $\Sigma_{E'''} \subset \mathbb{N}$  – полное множество (алфавит) возможных весов ребер графа  $G'''$ .  
 $\ell_{E'''} : E''' \rightarrow \Sigma_{E'''}$  – отображение, описывающее задание весов ребрам графа  $G'''$ .

На L7 в качестве вершин будем рассматривать только оконечные устройства, на которых работают приложения, взаимодействующие по сети. Дуги отражают наличие хотя бы одного такого взаимодействия некоторой направленности между элементами. Тогда КСПТП на L7 представим в виде ориентированного мультиграфа без петель: упорядоченной пары

$$G''' = (V''', E'''),$$

где  $V'''$  – множество вершин графа такое, что:

$$V''' \subset V''$$

(и соответственно

$$V'''' \subset V''', V'''' \subset V', V'''' \subset V); \\ V'''' = P, n'''' = |P|.$$

$E''''$  – множество дуг, соответствующих связям по передаче некоторой информации (в том числе служебной) между приложениями на устройствах. Взаимодействие элементов КСПТП (например, информационный процесс) 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.

Для L3 вводятся ограничения, учитывающие веса ребер и необходимые для исключения из рассмотрения неприемлемых в силу особенностей функционирования устройств сети маршрутов по графу:

1. Взаимодействие между двумя элементами КСПТП отражается маршрутом с наименьшим весом. Данное правило обусловлено особенностями передачи локального трафика (не направляется на маршрутизатор и не передается через другие оконечные устройства). При выполнении данного правила между оконечными устройствами в рамках широковещательного домена всегда существует кратчайший путь с весом  $a$ . Также правило учитывает особенности работы протоколов маршрутизации.

2. В маршруте не могут одновременно присутствовать ребра с весом  $a$  и ребра с другими весами (оконечные устройства не могут взаимодействовать через иные оконечные устройства).

Уровни модели согласованы между собой. Можно рассматривать КСПТП, двигаясь по вертикали снизу вверх, например, при составлении модели некоторой КСПТП и сверху вниз, например, при представлении подсистем АИС на графах КСПТП. Некоторому элементу модели (вершине или ребру) на уровне  $n$  ставится в соответствие некоторое подмножество элементов модели на уровне  $n-1$  и ниже. Взаимодействие, происходящее на уровне  $n$ , отображается на уровне  $n$  модели и всех уровнях ниже  $n$ .

Создание уровневой модели КСПТП состоит из следующих этапов:

Шаг 1. Выделение основных множеств элементов заданной КСПТП.

Шаг 2. Определение элементов КСПТП, работающих на L1 (все элементы), и сопоставление им вершин графа L1. Определение физических соединений между элементами КСПТП, сопоставление им ребер графа, соединяющих соответствующие вершины. Построение графа L1.

Шаг 3. Определение элементов КСПТП, работающих на L2 и незаблокированных, и сопоставление им вершин графа канального уровня. Определение незаблокированных физических соединений между элементами КСПТП, сопоставление им ребер графа, соединяющих соответствующие вершины. Построение графа L2.

Шаг 4. Определение элементов КСПТП, работающих на L3, и сопоставление им вершин графа сетевого уровня. Определение непосредственных или через элементы КСПТП более низкого уровня связей между элементами КСПТП, сопоставление им ребер графа, соединяющих соответствующие вершины. Построение графа L3.

Шаг 5. Определение окончательных устройств в КСПТП и сопоставление им вершин графа L7. Определение связей по передаче информации между приложениями на данных устройствах. Если найдена хотя бы одна такая связь между данными элементами, это свидетельствует о наличии ребра между соответствующими вершинами графа. Построение графа L7.

Шаг 6. Отображение подсистемы АИС ПТП на графе уровня приложений (L7).

Конец алгоритма.

## ВЫВОДЫ

Методика построения уровневой графовой модели КСПТП позволяет на основе правил, разработанных авторами, получить

валидные подграфы подсистем АИС ПТП КСПТП, необходимые для построения СЗИ АИС ПТП. Кроме того, данная методика может быть автоматизирована.

## ЛИТЕРАТУРА

1. *Гайфуллин Б.Н.* Автоматизированные системы управления предприятиями стандарта ERP/MRP. – М.: Богородский печатник. С. 237.
2. *Мишин Д.В., Монахова М.М.* Об оптимизации администрирования КСПД в условиях ограниченных административных ресурсов // Вестник НТУ "ХПИ". Тематический выпуск: Информатика и моделирование. – 2011, №17. С. 101...108.
3. *Mishin D.V., Andreev A.V., Monakhova M.M.* The use of the priority model in optimization of corporate data network administrating // The Strategies of Modern Science Development: Proceedings of the International scientific-practical conference (Yelm, WA, USA, 29-30 March 2013). – Yelm, WA, USA: Science Book Publishing House, 2013. P. 3...11. ISBN 978-1-62174-024-7.

## REFERENCES

1. Gajfullin B.N. Avtomatizirovannye sistemy upravleniya predpriyatijami standarta ERP/MRP. – M.: Bogorodskij pechatnik. S. 237.
2. Mishin D.V., Monakhova M.M. Ob optimizacii administrirovanija KSPD v uslovijah ogranichennyh administrativnyh resursov // Vestnik NTU "HPI". Tematicheskij vypusk: Informatika i modelirovanie. – 2011, №17. S. 101...108.
3. Mishin D.V., Andreev A.V., Monakhova M.M. The use of the priority model in optimization of corporate data network administrating // The Strategies of Modern Science Development: Proceedings of the International scientific-practical conference (Yelm, WA, USA, 29-30 March 2013). – Yelm, WA, USA: Science Book Publishing House, 2013. P. 3...11. ISBN 978-1-62174-024-7.

Рекомендована кафедрой информатики и защиты информации. Поступила 06.06.18 .