

# ОБ УСТОЙЧИВОСТИ ФУНКЦИОНИРОВАНИЯ СЕТЕЙ ОБМЕНА УПРАВЛЯЮЩЕЙ ИНФОРМАЦИЕЙ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ИНФОКОММУНИКАЦИОННЫМИ СЕТЯМИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

**Щелков**

**Дмитрий Александрович,**

адъюнкт кафедры  
технологий и средств технического  
обеспечения и эксплуатации  
автоматизированных систем  
управления  
Военно-космической академии  
имени А.Ф. Можайского,  
г. Санкт-Петербург, Россия,  
Dmitry-Schelkov@yandex.ru

## Ключевые слова:

сети обмена управляющей  
информацией, протокол RIP,  
алгоритм Беллмана-Форда,  
протокол OSPF, алгоритм Дейкстры,  
состояния смежности.

АННОТАЦИЯ

Анализ потоков информации, циркулирующих в различных современных инфокоммуникационных системах и сетях специального назначения (ИКС СН) (в т.ч. в наложенных сетях обмена управляющей информацией автоматизированных систем управления (АСУ) инфокоммуникационной сетью специального назначения), реализующих Internet protocol (IP), показывает наличие значительного числа сообщений различных видов, передаваемых в виде IP-пакетов. Среди многообразия задач, решаемых в процессе функционирования таких сетей, можно выделить основную – обеспечение передачи заданного объема потоков управляющих сообщений с заданной своевременностью, достоверностью при обеспечении требуемого уровня устойчивости в условиях фиксированного уровня ресурсов.

Как правило, сети обмена управляющей информацией АСУ инфокоммуникационными сетями специального назначения строятся путем наложения на некоторую транспортную основу слоя, реализующего Internet protocol (IP) или сочетание IP/MPLS.

Устойчивость информационного взаимодействия должностных лиц пунктов управления в настоящее время приобретает наиболее важное значение, так как процессы передачи информации в IP-сети с применением стандартных протоколов управления и маршрутизации не обеспечивают требуемый ее уровень в реальных условиях эксплуатации.

Традиционное объединение локальных сетей должностных лиц пунктов управления АСУ ИКС СН через слабо защищенную внешнюю среду передачи информации в единую сеть с образованием защищенной виртуальной сети, в которой каналы связи интерпретируются с помощью каналов связи реальной сети, не защищают от несанкционированных воздействий через протоколы маршрутизации и управления.

Известные методы снижения возможности несанкционированных воздействий на сеть при использовании в ней простого протокола сетевого управления SNMP рассмотрены в работе.

Поэтому актуальным является рассмотрение возможных вариантов обеспечения устойчивой работы сетей обмена управляющей информацией АСУ инфокоммуникационной сетью специального назначения, реализующих IP на сетевом уровне, при использовании в наложенной IP-сети наиболее часто применяемых протоколов маршрутизации RIP и OSPF.

Протокол RIP (Routing Information Protocol) описан в документе RFC 1058. Протокол RIP относится к классу протоколов IGP. Этот протокол является одним из первых протоколов обмена маршрутной информацией между маршрутизаторами в IP-сети и основывается на использовании алгоритма длины вектора. Впервые протокол RIP появился в 1982 году как часть стека протокола TCP/IP для UNIX. Исторически протокол RIP близко связан с семейством сетевых протоколов фирмы Херох. Преимуществом протокола RIP является его простота. Недостатком – увеличение трафика за счёт периодической рассылки широковещательных сообщений.

Этот алгоритм основывается на тех же принципах, что и алгоритм Беллмана-Форда, который был применён в первом протоколе маршрутизации для сетей ARPA и исходит из предположения, что каждый маршрутизатор может вычислить самый короткий маршрут и соответствующее расстояние до каждой сети. При применении его в сети каждый маршрутизатор выбирает ближайший соседний маршрутизатор, который расположен на этом самом коротком маршруте до получателя. Выбор осуществляется на основании информации о стоимости путей (выбирается путь с меньшей стоимостью). Стоимость вычисляется по информации, имеющейся в таблицах маршрутизации всех соседних маршрутизаторов. Маршрутизаторы регулярно обмениваются между собой таблицами маршрутизации. Протокол RIP использует в качестве метрики маршрута количество переходов, то есть число маршрутизаторов, которые должен миновать пакет (дейтаграмма), прежде чем он достигнет получателя. Маршрутизаторы с поддержкой протокола RIP всегда выбирают маршрут в сети с наименьшим числом переходов. На рис. 1. представлена метрика протокола RIP.

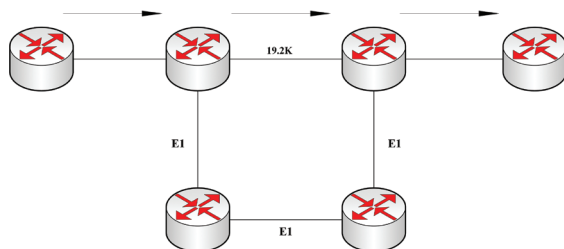


Рис. 1. Метрика протокола RIP

Маршрут с полосой пропускания равной 19,2 Кбит/с включает в себя три перехода. Нижний альтернативный маршрут по каналам связи E1 включает пять переходов. Поскольку выбор маршрута в протоколе RIP основывается на количестве переходов, то в данном случае в таблицу маршрутизации будет записан маршрут с пропускной способностью 19,2 Кбит/с вместо гораздо более быстрых каналов E1.

Протокол RIP предотвращает появление петель в маршрутизации, по которым пакеты могли бы циркулировать неопределенно долго, устанавливая максимально допустимое количество переходов на маршруте от отправителя к получателю. Стандартное максимальное

значение количества переходов равно 15. При получении маршрутизатором обновление маршрутов, содержащее новую или измененную запись, он увеличивает значение метрики на единицу. Ограничение в 15 транзитных узлов сужает область применения протокола RIP до сетей, в которых число промежуточных маршрутизаторов не должно превышать 15. Для более масштабных сетей нужно использовать другие протоколы маршрутизации, или разбивать сеть на автономные области.

К появлению новых маршрутов маршрутизаторы RIP приспособляются без труда: в очередном сообщении своим соседям они передают новую информацию, так что та постепенно становится известна всем маршрутизаторам сети. А вот к отрицательным изменениям, связанным с потерей какого-либо маршрута, им адаптироваться сложнее. Дело в том, что в формате сообщений протокола RIP нет поля, где бы содержалась информация об отсутствии пути к данной сети. Некоторый маршрут становится недействительным на основании истечения времени жизни маршрута или указания специального расстояния до сети. Для реализации первого механизма каждая запись таблицы маршрутизации, полученная по протоколу RIP, имеет время жизни (TTL). При поступлении очередного сообщения RIP с подтверждением того, что данная запись действительна, таймер TTL устанавливается в исходное состояние, а затем из него каждую секунду вычитается единица. Если за время тайм-аута не придет новое маршрутное сообщение об этом маршруте, то он отмечается как недействительный. Время ожидания связано с периодом рассылки векторов по сети. Период рассылки в RIP равен 30 с., а в качестве тайм-аута принято шестикратное значение периода рассылки. Шестикратный запас времени нужен для уверенности в том, что проблемы заключаются не в потерях сообщений RIP (а это возможно, так как RIP использует транспортный протокол UDP, который не гарантирует доставку сообщений), а в том, что сеть действительно стала недоступна. Если какой-либо маршрутизатор выходит из строя, то через 180 с все порожденные этим маршрутизатором записи станут недействительными у его ближайших соседей. После этого процесс повторится уже для ближайших соседей – они вычеркнут подобные записи через 360 с, так как первые 180 с ближайшие соседи еще передавали сообщения об этих записях. Как видим, сведения о недоступных через отказавший маршрутизатор сетях распространяются по сети не очень быстро, время распространения кратно времени жизни записи, а коэффициент кратности равен количеству транзитных узлов между самыми дальними маршрутизаторами сети. В этом и заключается одна из причин выбора в качестве периода рассылки небольшой величины.

Так как протокол RIP был разработан достаточно давно и практически не изменялся за это время, он обладает определенными недостатками, которые ограничивают его применение в достаточно сложных сетях [2], но в сети обмена управляющей информацией автоматизированных систем управления (АСУ) инфоком-

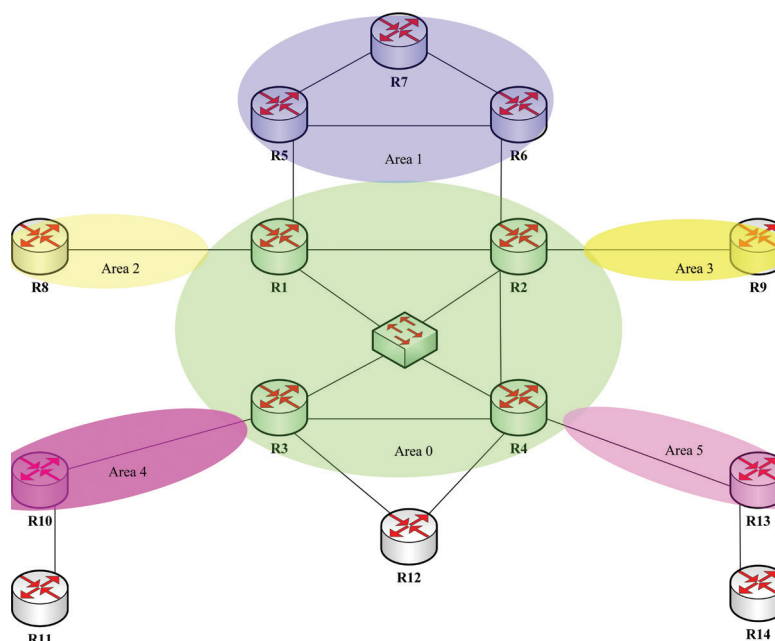


Рис. 2. Разбиение автономной системы на несколько областей

муникационной сетью специального назначения он может быть достаточно хорош.

Существует спецификация протокола OSPF (Open Shortest Path First), которая описана в документе RFC 1247. Протокол OSPF использует деление автономной системы на несколько областей, в каждой из которых работает своя копия протокола. Деление автономной системы на несколько областей позволяет значительно сократить нагрузку на сеть. Пример разбиения системы на области представлен на рис. 2.

Протокол OSPF может вычислять маршруты в сети, работая совместно с другими протоколами обмена маршрутной информацией. Данный протокол основан на алгоритме состояния канала. Суть этого алгоритма состоит в том, что необходимо вычислить кратчайший путь. При этом «кратчайший» не означает, что путь физически самый короткий. Имеется в виду что, информация пройдёт по этому пути быстрее, чем по другим. Маршрутизатор сети, работающий с этим протоколом, отправляет запросы всем соседним маршрутизаторам, находящимся в одном с ним домене маршрутизации, для выявления состояния каналов до них и далее от них. Состояние канала при этом характеризуется несколькими параметрами, которые называются метриками. Метрикой может быть пропускная способность канала, его загрузка на текущий момент, задержка информации при её прохождении по этому каналу и т.д. Обобщив полученные сведения, этот маршрутизатор сообщает их всем соседям. После этого им строится ориентированный граф, который повторяет топологию домена маршрутизации. Каждому ребру этого графа назначается оценочный параметр (метрика) рис. 3.

После построения графа используется алгоритм Дейкстры, который по двум заданным узлам находит

набор рёбер с наименьшей суммарной стоимостью, т.е. по сути, выбирает оптимальный маршрут. По совокупной информации (полученной и найденной в результате вычислений) создаётся таблица маршрутизации.

Протокол OSPF состоит из трёх внутренних подпротоколов: Hello, Exchange, Flooding. Периодически маршрутизаторы сети обмениваются между собой сообщениями подпротокола Hello. Важным процессом в протоколе OSPF является установка связей между маршрутизаторами. Протокол OSPF имеет несколько состояний. Самое простое состояние, при котором не происходит обмен между соседними маршрутизаторами, обычно наблюдается сразу после подключения к сети маршрутизатора, работающего под управлением протокола OSPF, или после возникновения нарушения в работе. Следующее состояние называется

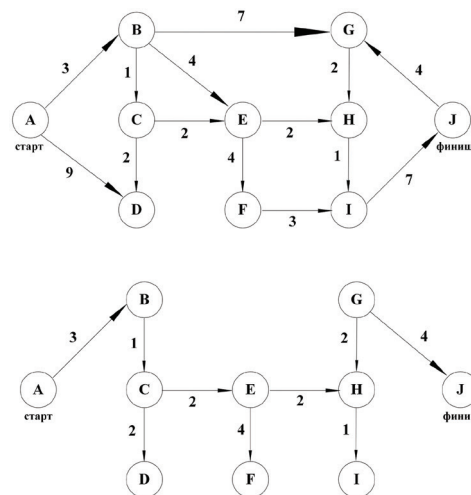


Рис. 3. Оценочные параметры рёбер графа

состоянием инициализации. В ходе данного состояния маршрутизатор OSPF посылает Hello пакеты для установки связи между соседними устройствами. В состоянии двусторонней связи каждый маршрутизатор OSPF пытается установить связь со всеми своими соседями, это происходит также с помощью пакета Hello. В данном пакете передаётся список всех известных соседних маршрутизаторов. Если маршрутизатор принимает пакет Hello и «видит» в этом пакете свой идентификатор, то считается что состояние двусторонней связи установлено. После установления связей маршрутизаторы переходят в послестартовое состояние. Это состояние представляет собой первый этап формирования отношений смежности, на котором необходимо определить, какой маршрутизатор должен быть ведущим и какой — ведомым. Ведущим становится маршрутизатор с наибольшим идентификатором. Ведущий маршрутизатор управляет процессом обмена данными, устанавливая и наращивая начальный порядковый номер базы данных. Ведущий и ведомый маршрутизаторы представлены на рис. 4.

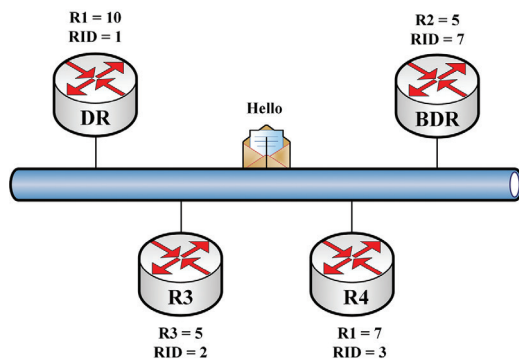


Рис. 4. Ведущий и ведомый маршрутизаторы

В следующем состоянии происходит обмен информацией о состоянии каналов. После получения маршрутизатором такой информации он сравнивает её со своей базой данных и если такая информация отсутствует, то маршрутизатор запрашивает полную информацию о данном канале. В следующем состоянии, которое называется состоянием загрузки, передача пакетов базы данных должна быть завершена, а соседнему устройству переданы пакеты запросов состояния каналов (Link-State request – LSR), содержащие требование передать более свежие анонсы, которые еще не были получены в состоянии обмена. В результате выполнения этих запросов передаются анонсы LSA, позволяющие завершить обмен информацией о маршрутах. После того как каждый маршрутизатор имеет свою таблицу смежных маршрутизаторов, считается что установлено состояние полной смежности. В данном состоянии маршрутизаторы приступают к нормальной работе.

В целом протокол OSPF и многие другие (IGRP, EIGRP, EGP, BGP, IGMP, DVMRP, MOSPF, PIM) подходят для современных больших, динамически изменяющихся сетей. Однако, ориентировка этих протоколов на от-

крытую сеть типа Интернет, предполагающая фактически знание на каждом маршрутизаторе всей структуры сети и возможность влияния на процессы маршрутизации извне, являются существенными недостатками. Поэтому применение их в сетях обмена управляющей информацией АСУ инфокоммуникационной сетью специального назначения, реализующих Internet protocol нежелательно по причинам невозможности обеспечения требований по качеству и безопасности.

Поэтому необходимы дополнительные приемы, разработаны алгоритмы усовершенствования, основанные на изменении формирования метрик при составлении матрицы маршрутов в маршрутизаторах сетей обмена управляющей информацией АСУ инфокоммуникационной сетью специального назначения. Эти алгоритмы должны учитывать особенности применяемых протоколов как IP, так RIP и OSPF. Эти алгоритмы, очевидно можно использовать. Причем процедуры формирования метрики можно распространить на каждый из доменов маршрутизации, что позволит организовать псевдоключевые зоны на сетевом уровне IP-сети. Эти алгоритмы должны быть встроены в стандартные протоколы маршрутизации (RIP и OSPF). Процедуры формирования метрики могут носить различный характер, определяемый степенью ее адекватности реальным процессам передачи информации в сети. Важно только то, чтобы они существенно отличались от применяемых в протоколах. При этом могут быть рекомендованы достаточно известные методы управления и формирования метрики [5].

Так, например, в процедуре вычисления метрики протокола RIP, в котором учитывается величина длины пути в числе транзитов  $R_i = \sum r_i$ , можно так изменить параметр  $r_i$ , чтобы он каким либо образом учитывал уровень нагрузки (или задержки пакета), т.е.  $r_{in} = r_i + \Delta r_i$ , причем  $\Delta r_i = f(r_{zi})$  или  $\Delta r_i = f_1(\rho_i)$ .

Аналогично, в процедуре вычисления метрики протокола OSPF, в котором учитывается пропускная способность исходящих из узлов сети трактов  $P_i = \sum y(p_i)$ , можно также изменить параметру  $y(p_i)$ , чтобы он определенным образом учитывал уровень нагрузки (или задержки пакета), т.е.  $y_n(p_i) = y(p_i) + y(\Delta p_i)$ , причем  $y(\Delta p_i) = f_y(t_{zi})$  или  $y(\Delta p_i) = f_{y1}(\rho_i)$ .

Вопросы учета степени влияния добавок  $\Delta r_i$  от величин  $t_{zi}$  или  $\rho_i$  являются достаточно сложными и требуют отдельных исследований. Важно, что такой подход позволяет учесть данные параметры, устранить недостатки приведенных известных протоколов и повысить показатели передачи в сети обмена управляющей информацией АСУ.

### Литература

1. Буренин А.Н., Легков К.Е. К вопросу управления современными инфокоммуникационными сетями, функционирующими в условиях интенсивных воздействий // Сборник трудов Северо-Кавказского филиала Московского технического университета связи

и информатики. Часть 1. Ростов-на-Дону.: ПЦ «Университет» СКФ МТУСИ, 2014. С. 101–103.

2. Легков К.Е., Буренин А.Н. Модели организации информационной управляющей сети для системы управления современными инфокоммуникационными сетями // Научные исследования в космических исследованиях Земли. 2012. Т. 4. № 1. С. 14–16.

3. Буренин А.Н., Легков К.Е. Эффективные методы

управления потоками в защищённых инфокоммуникационных сетях // Научные исследования в космических исследованиях Земли. 2010. Т. 2. № 2. С. 29–34.

4. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. СПб.: БХВ-Петербург. 2000. 512 с.

5. Буренин А.Н. Об управлении маршрутизацией на основе модифицированных адаптивных методов // Техника средств связи. Сер. ТПС. 1991. № 7. С. 51–59.

#### Для цитирования:

Щелков Д.А. Об устойчивости функционирования сетей обмена управляющей информацией автоматизированных систем управления инфокоммуникационными сетями специального назначения // Научные исследования в космических исследованиях Земли. 2015. Т. 7. № 5. С. 24–28.

#### ABOUT THE SUSTAINABILITY OF EXCHANGE NETWORKS OF MANAGEMENT INFORMATION AUTOMATED SYSTEMS MANAGEMENT INFO-COMMUNICATION NETWORKS SPECIAL PURPOSE

**Shchelkov Dmitry Aleksandrovich,**

St. Petersburg, RussianDmitry-Schelkov@yandex.ru

#### Abstract

The analysis of flows of information circulating in various modern infocommunication system and networks (ICN SP) (including in the imposed networks of an exchange of operating information of automatic control system (ACS) an infocommunication network of a special purpose), realizing IP, shows existence of considerable number of messages of the different types transferred in the form of IP of packages.

Among variety of the tasks solved in the course of functioning of such networks, it is possible to allocate the main - ensuring transfer of the set volume of flows of operating messages with the set timeliness, reliability when providing demanded level of stability in the conditions of the fixed level of resources.

As a rule, networks of an exchange of operating information of ACS infocommunication networks of a special purpose are under construction by imposing on some transport basis of the layer realizing IP or a combination of IP/MPLS.

Stability of information interaction of officials of points of management gets now most importance as information transfer processes in an IP network with application of standard protocols of management and routing level demanded it in actual practice does not provide operation.

Traditional association of the ACS ICN SP local networks through poorly protected environment of information transfer in a uniform network with formation of the protected virtual network in which communication channels are interpreted by means of communication channels of a real network, do not protect from unauthorized influences through routing and management protocols.

Known methods of decrease in possibility of unauthorized impacts on a network when using in it the simple protocol of network management of SNMP are considered in work.

Therefore consideration of possible options of ensuring steady work of networks of an exchange by operating information of ACS by an infocommunication network of the special purpose, realizing IP at network level is actual, when using in the imposed IP network of most often applied protocols of routing of RIP and OSPF.

**Keywords:** the network exchange control information, RIP, the algorithm of Bellman-Ford, OSPF, Dijkstra's algorithm, the state of the adjacency.

#### References

1. Burenin A.N., Legkov K.E. To a question of management of the modern infocommunication networks functioning in the conditions of intensive influences. In collection of works of the North Caucasian branch of the Moscow technical university of communication and informatics. Part 1. Rostov-on-Don.: PTs SKF "University" MTUSI. 2014. Pp. 101–103. (in Russian).

2. Legkov K.E., Burenin A.N. Models of the organization of the information managing director of a network for management system the modern infocommunication networks. H&ES Research. 2012. Vol. 4. No.1. Pp. 14–16. (in Russian).

3. Burenin A.N., Legkov K.E. Effective methods of control over flows on the protected infocommunication networks. H&ES Research. 2010. Vol. 2. No. 2. Pp. 29–34. (in Russian).

4. Olfier V. G., Olfier N. A. Novye tekhnologii i oborudovanie IP-setey [New technologies and equipment of IP networks]. SPb. BHV Petersburg. 2000. 512 p. (in Russian).

5. Burenin A.N. About management of routing on the basis of the modified adaptive methods. Tekhnika sredstv svyazi. Ser. TPS. 1991. No. 7. Pp. 51–59. (in Russian).

#### Information about authors:

Shchelkov D.A. post-graduate student of the Department automated systems of control, Military Space Academy.

#### For citation:

Shchelkov D.A. About the sustainability of exchange networks of management information automated systems management info-communication networks special purpose. H&ES Research. 2015. Vol. 7. No. 5. Pp. 24–28. (in Russian).