УДК 004.05

***В.В. Бухарин, С.Ю. Карайчев***
(Академия Федеральной службы охраны Российской Федерации;
e-mail: bobah_buch@mail.ru)

# МЕТОД ЗАЩИТЫ ИНФОРМАЦИОННОГО ОБМЕНА СЕГМЕНТОВ РАСПРЕДЕЛЁННОЙ МУЛЬТИСЕРВИСНОЙ СЕТИ

*Разработан метод защиты информационного обмена сегментов распределённой мультисервисной сети за счёт использования модифицированной процедуры определения используемых адресов.*

*Ключевые слова: мультисервисная сеть, деструктивные воздействия, адреса отправителя и получателя, информационный обмен.*

***V.V. Buharin, S.Y. Karaichev***

# METHOD OF PROTECTION OF INFORMATION EXCHANGE OF SEGMENTS OF THE DISTRIBUTED MULTISERVICE NETWORK

*The method of protection of information exchange of segments of the distributed multiservice network due to use of the modified procedure of definition of the used addresses was designed.*

*Key words: multiservice network, destructive influences, addresses of the sender and recipient, information exchange.*

Статья поступила в редакцию Интернет-журнала 15 июня 2015 г.

При объединении удалённых сегментов распределённой ***мультисервисной сети (МСС)*** через сети связи общего пользования (например, Интернет) усложняется решение задачи по обеспечению безопасности связи. Это связано с возникновением значительного спектра потенциальных угроз, связанных либо с несанкционированным доступом к информации или её перехватом в процессе передачи по каналам связи, либо деструктивными воздействиями на МСС. Задача защиты информационной части пакетов сообщений достаточно эффективно решается средствами криптографии. Однако даже при отсутствии возможности декодирования перехваченной информации нарушитель путём анализа сетевого трафика (заголовков пакетов сообщения) имеет возможность определить информационное взаимодействие сегментов распределённой МСС. Это обусловлено тем, что заголовки пакетов сообщений передают в открытом виде.

Основными данными из заголовка пакета сообщения, используемыми для определения информационного взаимодействия, являются адреса отправителей, получателей и идентификатор пакета сообщения. *IP*-адреса представляют собой основной тип адресов, на основании которых осуществляют передачу пакетов между сетями. Эти адреса состоят из последовательности в 32 бита. *IP*-адрес назначает администратор, и он состоит из двух частей: номера сети и номера узла. Всё пространство адресов делится на пять классов, в соответ-

ствии с которыми определяется, сколько бит адреса относится к сетевой части, а сколько – к узловой. При маршрутизации пакета через внешние сети основную роль играет сетевая часть *IP*-адреса, так как на промежуточных маршрутизаторах направление передачи пакета определяется по номеру сети (сетевая часть *IP*-адреса) [1].

При передаче пакета источник присваивает ему идентификационный номер размером 16 *бит*. Данный номер используется в случае выполнения фрагментации пакета при прохождении через внешнюю сеть. Все фрагменты пакета будут иметь одинаковый идентификационный номер. Это необходимо для правильной сборки фрагментов в исходный пакет [2]. При информационном взаимодействии сегментов распределённой МСС номерование пакетов будет осуществляться последовательно.

Таким образом, для обеспечения безопасности и скрытности работы сегментов распределённой МСС по каналам связи возникает необходимость использования процедуры скрытия истинных адресов корреспондентов и изменение значений идентификаторов пакетов в информационном потоке сообщений.

Реализацию предложенного метода можно пояснить на схеме МСС, показанной на рис. 1. Сегменты распределённой МСС 1.1 и 1.2 подключены к внешней сети 2 посредством маршрутизатора 1.1.3 и 1.2.3. В общем случае сегмент распределённой МСС 1.1 представляет собой совокупность ПЭВМ $1.1.1_1$-$1.1.1_N$, периферийного и коммуникационного оборудования 1.1.2 и 1.1.3, объединённого физическими линиями связи. Все эти элементы имеют идентификаторы, в качестве которых в наиболее распространённом стеке протоколов *TCP*/*IP* используются сетевые адреса (*IP*-адреса).

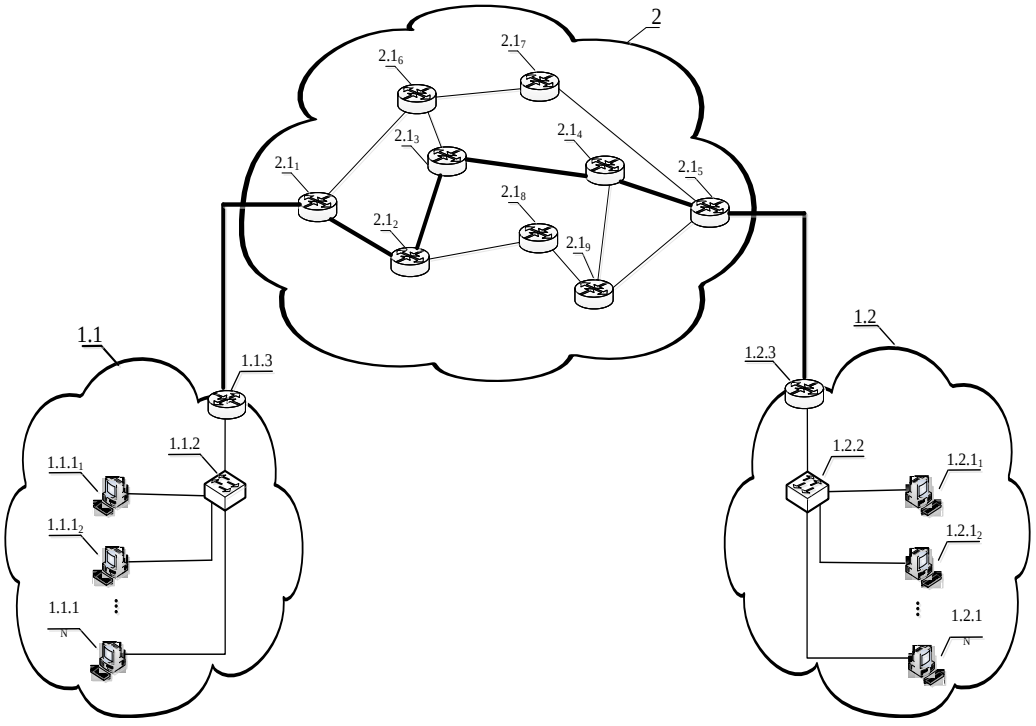


**Рис. 1.** Структура распределённой мультисервисной сети

Внешняя сеть представлена набором маршрутизаторов $2.1_1$-$2.1_9$, осуществляющих транспортировку информационных потоков из одного сегмента распределённой МСС в другой.

Структура пакетов сообщений известна, как известен и принцип передачи пакетов в вычислительных сетях. Например, на рис. 2 представлена структура заголовка *IP*-пакетов сообщений, где выделены поля: идентификатор, адреса отправителя и получателя пакета сообщений [3]. При прохождении пакетов через внешнюю сеть осуществляется его маршрутизация от источника к получателю в соответствии с *IP*-адресом назначения.

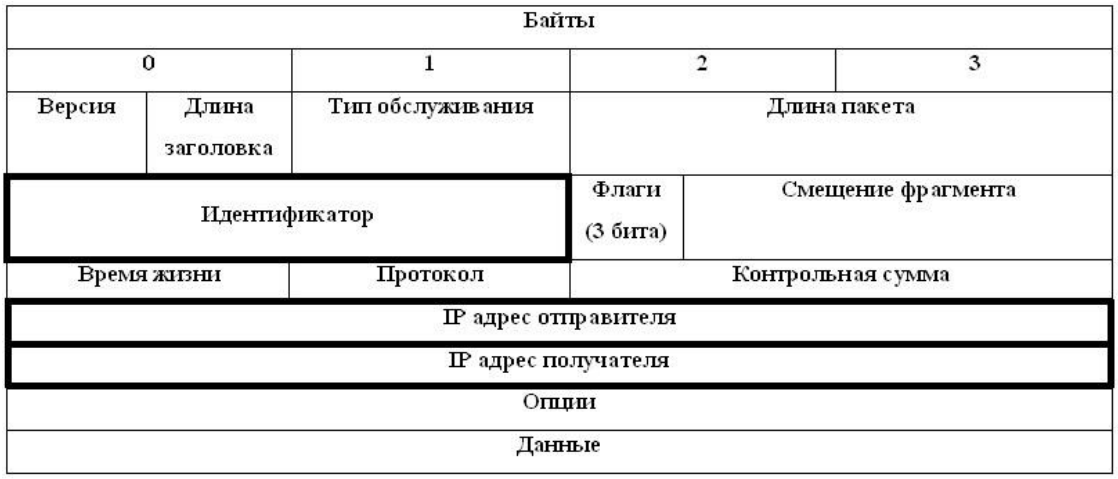


**Рис. 2.** Структура IP-заголовка пакета сообщений

На рис. 3 представлена схема, поясняющая процесс передачи и приёма информационного и уведомляющего пакетов сообщений, а на рис. 4 – последовательность действий, реализующих метод защиты информационного обмена сегментов распределённой МСС.

На начальном этапе задают исходные данные, включающие адреса отправителя и получателя сообщений. Формируют у получателя и отправителя в предварительно заданные исходные данные базу из $Z$ ложных адресов отправителя. После чего запоминают текущие адреса отправителя и получателя (блок 1-3, рис. 4).

Выделяют из заданной базы ложных адресов текущий ложный адрес отправителя $A_{\text{отпр}}^{\text{лож}}$ и запоминают его. Формируют идентификатор заголовка пакета $ID_{\text{случ}}$ по случайному закону (блок 4-6, рис. 4).

У отправителя из предварительно заданной базы ложных адресов отправителя случайным образом выделяют обратный ложный адрес отправителя $A_{\text{отпр}}^{\text{об лож}}$ и запоминают его (блок 7, рис. 4).

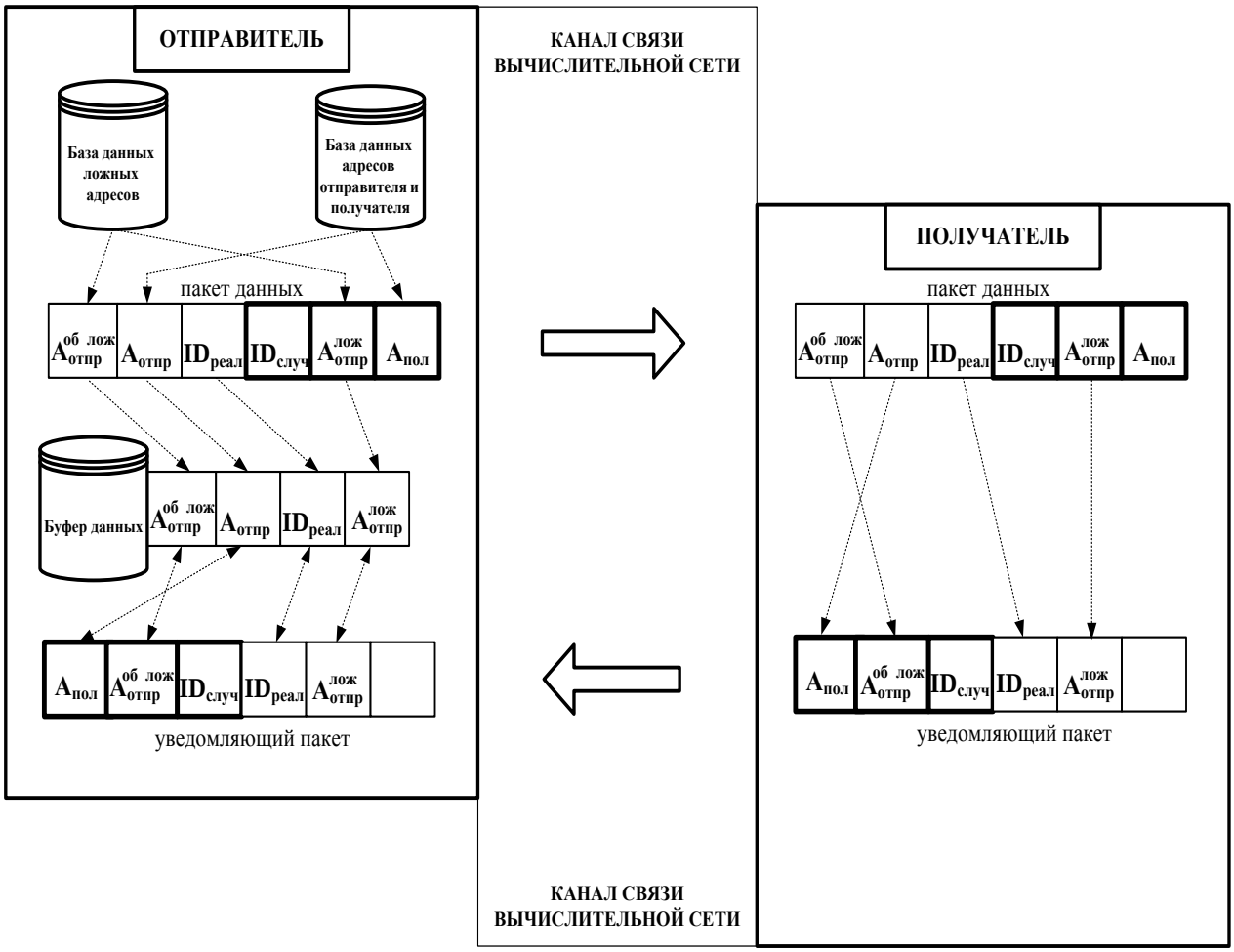


**Рис. 3.** Схема передачи и приёма информационного и уведомляющего пакетов сообщений

Первоначально у отправителя формируют исходный пакет данных, в который включают предварительно запомненные текущий адрес отправителя $A_{\text{отпр}}$ и обратный ложный адрес отправителя $A_{\text{отпр}}^{\text{об лож}}$, а также реальный идентификатор пакета $ID_{\text{реал}}$. После чего кодируют любым из известных способов кодирования [4] и преобразуют его в формат *TCP*/*IP* (блок 8-11, рис. 4). Преобразование заключается в добавлении *IP*-заголовка к кодированному пакету данных. Полученный в результате пакет является информационным пакетом сообщения, в котором заменены текущий адрес отправителя $A_{\text{отпр}}$ на предварительно запомненный ложный текущий адрес отправителя $A_{\text{отпр}}^{\text{лож}}$, и реальный идентификатор заголовка пакета $ID_{\text{реал}}$ на сформированный идентификатор $ID_{\text{случ}}$ по случайному закону, а в качестве адреса получателя используется текущий адрес получателя $A_{\text{пол}}$. Передают получателю сформированный информационный пакет сообщений (блок 12-13, рис. 4).

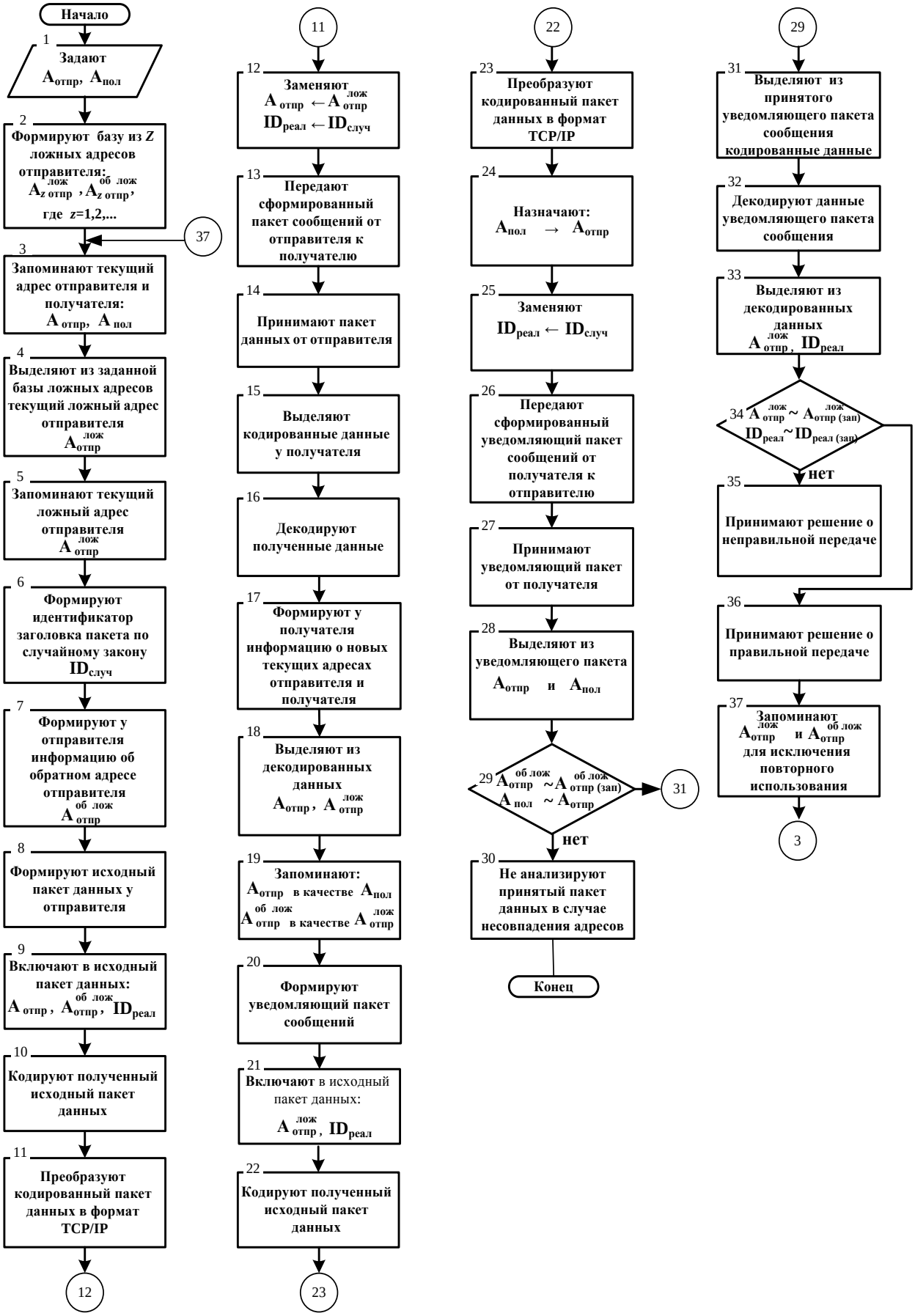


**Рис. 4.** Последовательность действий метода защиты информационного обмена сегментов распределённой МСС

На втором этапе, после приёма у получателя информационного пакета сообщения выделяют кодированные данные и декодируют их (блок 14-16, рис. 4). Далее формируют у получателя информацию о новых текущих адресах отправителя и получателя. Для этого выделяют из декодированных данных текущий адрес отправителя $A_{\text{отпр}}$, который используют в качестве текущего адреса получателя $A_{\text{пол}}$, и обратный ложный адрес отправителя $A_{\text{отпр}}^{\text{об лож}}$, который используют в качестве текущего ложного адреса отправителя $A_{\text{отпр}}^{\text{лож}}$, и запоминают их (блок 17-19, рис. 4).

На третьем этапе для подтверждения факта получения от отправителя пакета, у получателя формируют уведомляющий пакет сообщения. Для чего аналогично, как и у отправителя формируют исходный пакет, представляющий собой уведомление о получении информационного пакета сообщения. Затем в исходный пакет включают предварительно запомненные текущий ложный адрес отправителя $A_{\text{отпр}}^{\text{лож}}$ и реальный идентификатор заголовка пакета $ID_{\text{реал}}$ (блок 20-21, рис. 4). Далее кодируют пакет данных и преобразуют его в формат *TCP*/*IP* (блок 22-23, рис. 4). Назначают текущим адресом отправителя $A_{\text{отпр}}$ предварительно запомненный обратный ложный адрес отправителя $A_{\text{отпр}}^{\text{об лож}}$, полученный из принятого от отправителя пакета сообщения. Также назначают текущим адресом получателя $A_{\text{пол}}$ предварительно запомненный адрес отправителя $A_{\text{отпр}}$ (блок 24, рис. 4). После этого заменяют реальный идентификатор заголовка пакета $ID_{\text{реал}}$ на сформированный идентификатор $ID_{\text{случ}}$ по случайному закону (блок 25, рис. 4). Далее передают сформированный уведомляющий пакет сообщения от получателя к отправителю (блок 26, рис. 4).

На четвёртом этапе, после приёма у отправителя уведомляющего пакета сообщения, из заголовка пакета выделяют текущие адреса отправителя $A_{\text{отпр}}^{\text{об лож}}$ и получателя $A_{\text{пол}}$ (блок 27-28, рис. 4). Сравнивают соответствующие адреса с предварительно запомненными обратным ложным адресом отправителя $A_{\text{отпр}}^{\text{об лож}}$ и адресом отправителя $A_{\text{отпр}}$ (блок 29, рис. 4). При несовпадении адресов принятый пакет сообщения не анализируют, а при совпадении выделяют из принятого уведомляющего пакета сообщения кодированные данные и декодируют их (блок 30-32, рис. 4).

Выделяют из декодированных данных текущий ложный адрес отправителя $A_{\text{отпр}}^{\text{лож}}$ и реальный идентификатор заголовка пакета $ID_{\text{реал}}$ (блок 33, рис. 4). Сравнивают выделенный текущий ложный адрес отправителя $A_{\text{отпр}}^{\text{лож}}$ и реальный идентификатор $ID_{\text{реал}}$ с соответствующими предварительно запомненными ложным адресом отправителя $A_{\text{отпр}}^{\text{лож}}$ и реальным идентификатором пакета $ID_{\text{реал}}$ (блок 34, рис. 4).

При несовпадении соответствующих адресов принимают решение о неправильной передаче пакета сообщения, а при совпадении – о правильной передаче (блок 35-36, рис. 4). Запоминают ложный адрес отправителя $A_{\text{отпр}}^{\text{лож}}$ и обратный ложный адрес отправителя $A_{\text{отпр}}^{\text{об лож}}$ для исключения повторного их использования (блок 37, рис. 4).

Таким образом, предлагаемый метод защиты за счёт использования модифицированной процедуры определения используемых адресов при информационном обмене между удалёнными сегментами МСС, путём введения ложных адресов из адресного пространства сетей, не относящихся к сегментам распределённой МСС, и изменения реальных идентификаторов передаваемых пакетов, позволяет повысить уровень безопасности и скрытности работы сегментов МСС по каналам связи [5].

## Литература


1. ***Олифер В.Г., Олифер Н.А.*** Компьютерные сети: Принципы, технологии, протоколы: учебник для вузов. СПб.: Питер, 2010. 944 с.

2. ***Золотов С.*** Протоколы Internet. СПб.: BHV-Санкт-Петербург, 1998. 304 с.

3. ***RFC 791***, Internet Protocol, 1981, сентябрь. С. 11-22.

4. ***Молдовян Н.А. и др.*** Криптография: от примитива к синтезу. СПб.: БВХ-Петербург, 2004. 446 с.

5. ***Пат. 2490703.*** Российская Федерация, МПК G06F 21/00. Способ защиты канала связи вычислительной сети / Бухарин В.В. и др.; ГКВОУ ВПО "Военная академия связи". № 2012123121/08. Заявл. 04.06.2012. Опубл. 20.08.2013. Бюл. № 23. 11 с.