УДК 004.738.5.057.4

В.В. Бухарин, А.В. Кирьянов, О.А. Баленко
(Военная академия связи; e-mail: bobah_buch@mail.ru)

МЕТОД ОБНАРУЖЕНИЯ ПОДМЕНЫ ДОВЕРЕННОГО ОБЪЕКТА ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Разработан метод обнаружения подмены доверенного объекта информационно-вычислительной сети. Метод позволяет повысить достоверность обнаружения подлога компьютерных адресов отправителя и получателя сетевых дейтаграмм.

Ключевые слова: программное обеспечение, компьютерные атаки, адреса отправителя и получателя.

V.V. Buharin, A.V. Kirianov, O.A. Balenko

THE METHOD OF DETECTION OF SUBSTITUTION OF THE ENTRUSTED OBJECT OF THE INFORMATION NETWORK

The method of detection of substitution of the entrusted object of an information network is offered. The method allows to raise reliability of detection of forgery of computer addresses of the sender and the receiver of network datagrams.

Key words: the software, computer attacks, addresses of the sender and the addressee.

В настоящее время ***информационно-вычислительные сети (ИВС)*** имеют множество уязвимостей, возникших при разработке системного программного обеспечения и неправильной конфигурации оборудования. Наличие угроз безопасности в ИВС делает реальным возможность злоумышленникам проводить различные виды атак. Границы информационно-вычислительной сети определяются не установленным оборудованием, а уровнем защищенности сети. В настоящее время наиболее часто реализуемые компьютерные атаки классифицируются на [1]:

- анализ сетевого трафика;
- сканирование сети;
- угроза выявления пароля;
- подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа;
- навязывание ложного маршрута сети;
- внедрение ложного объекта сети;
- отказ в обслуживании;
- удаленный запуск приложений.

Для противодействия злоумышленникам ИВС должна иметь иерархическую и системно-взаимоувязанную защиту. Вышеперечисленные компьютерные атаки могут влиять на достоверность получаемой информации, в связи с чем актуальной является задача обнаружения подмены доверенного объекта ИВС.

Известен способ организации локальной компьютерной сети и межсетевого экрана [2], заключающийся в том, что защита внутренней сети обеспечивается с помощью межсетевого экрана, представляющего собой комплекс аппаратных и программных средств, содержащий, по меньшей мере, два сетевых интерфейса для обмена двунаправленными потоками сетевых пакетов между сетевыми интерфейсами межсетевого экрана и осуществляющий фильтрацию транслируемых сетевых пакетов в соответствии с заданными правилами. При этом межсетевой экран исключён из числа абонентов сети путём такой настройки программы его управления, при которой эта программа использует для приёма и передачи пакетов сетевые интерфейсы межсетевого экрана без назначения им логических адресов, скрывает информацию об их физических адресах, а задание правил фильтрации осуществляется с помощью отдельного интерфейса управления, не имеющего связи с сетевыми интерфейсами межсетевого экрана.

Однако этот способ имеет недостатки, заключающиеся в отсутствии механизмов контроля сетевых дейтаграмм внутри защищаемой сети, возможности посылки сетевых дейтаграмм с подложным адресом отправителя сетевой дейтаграммы, а также возможности беспрепятственного перехвата и модификации содержимого сетевых дейтаграмм.

Известен способ межсетевого экранирования [3], сущность которого заключается в децентрализации средств межсетевого экранирования путем установки межсетевых экранов на все компьютеры защищаемой сети и синхронизации правил фильтрации сетевых дейтаграмм через единый выделенный сервер. При этом на защищаемых компьютерах дублируются правила и функции средств межсетевого экранирования, а синхронизация производится через сетевую службу удаленного управления единым реестром записей ОС Windows.

Недостатки данного способа связаны с высокой вычислительной нагрузкой на защищаемые компьютеры, необходимостью развертывания и эксплуатации выделенного сервера для синхронизации правил фильтрации сетевых дейтаграмм, малой эффективностью фильтрации в случае необходимости быстрого реагирования на компьютерные атаки.

Наиболее близким по технической сущности к предлагаемому способу является способ обработки дейтаграмм сетевого трафика для разграничения доступа к информационно-вычислительным ресурсам компьютерных сетей [4]. Способ заключается в следующих действиях: для защиты вычислительных сетей используют шлюз-компьютер с межсетевым экраном, межсетевой экран проверяет сетевые дейтаграммы в соответствии с заданным оператором списком правил доступа в компьютерную сеть, записывает в дейтаграммах пометки, соответствующие правилам доступа, затем осуществляет прозрачную ретрансляцию корректных дейтаграмм, а на стороне получателя пропускает или блокирует сетевые дейтаграммы в соответствии с указанными внутри пометками.

Недостатком данного способа является низкая достоверность обнаружения подлога компьютерных адресов отправителя и получателя сетевых дейтаграмм, обусловленная выполнением соответствующих действий по обнаружению подмены только в локальной защищённой сети, при этом не учитывается возможность подмены во внешней сети и соответственно возможность несанкционированного проникновения в защищаемую информационно-вычислительную сеть.

Целью заявленных авторами настоящей статьи технических решений является разработка метода обнаружения подмены доверенного объекта информационно-вычислительной сети, обеспечивающего повышение достоверности обнаружения подлога компьютерных адресов отправителя и получателя сетевых дейтаграмм за счет скрытия истинных адресов отправителя и получателя сетевых дейтаграмм путем шифрования сетевых дейтаграмм и последовательной передачи между доверенными узлами информационно-вычислительной сети в соответствии с информацией о маршруте передачи.

Реализация данного метода осуществляется следующим образом:

В качестве ИВС рассматривается сеть, состоящая из маршрутизаторов 1 внешней сети 3 и доверенных узлов 2, на которых используют шлюз-компьютер с межсетевым экраном. Порядок передачи сетевой дейтаграммы от абонента S_A к абоненту S_B в заявленном способе поясняется на рис. 1 и описан алгоритмом на рис. 2.

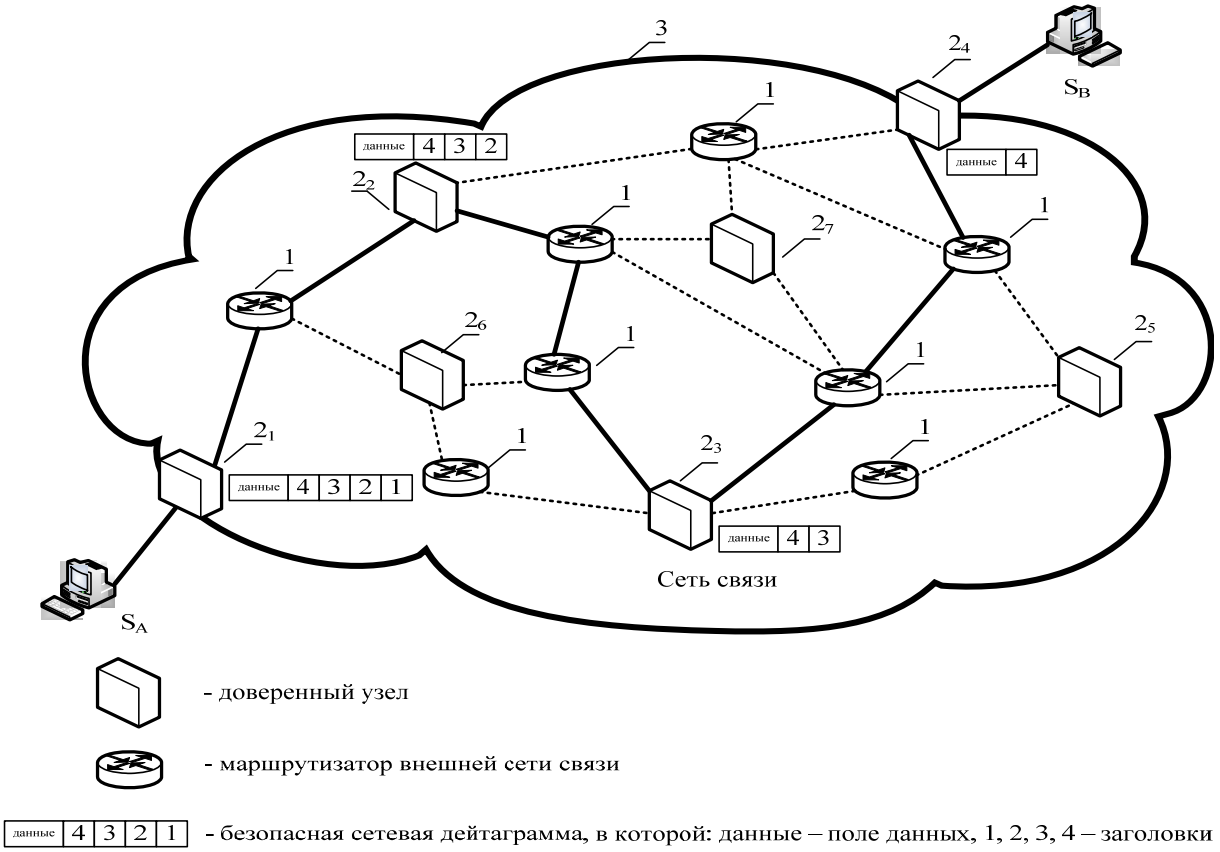


Рис. 1. Схема порядка формирования маршрута передачи пакетов сообщений в ИВС

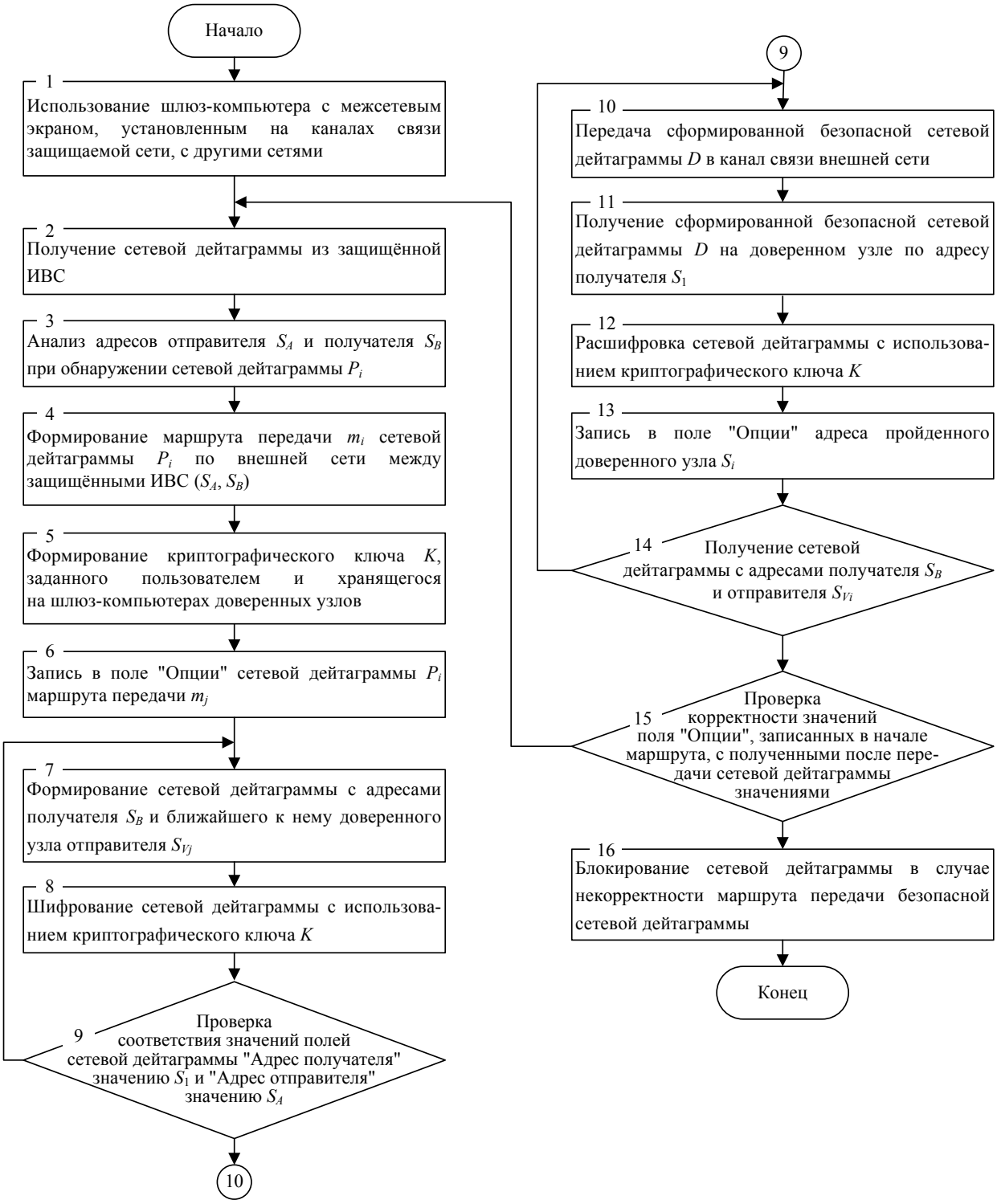


Рис. 2. Блок-схема алгоритма обработки дейтаграмм сетевого трафика для защиты ИВС

На рис. 3 поясняется порядок формирования безопасной сетевой дейтаграммы при передаче по маршруту m_1, включающем четыре доверенных узла 2. Первый пакет – от $П_1$ является исходным, в его заголовке указаны адреса отправителя S_A и получателя S_B.

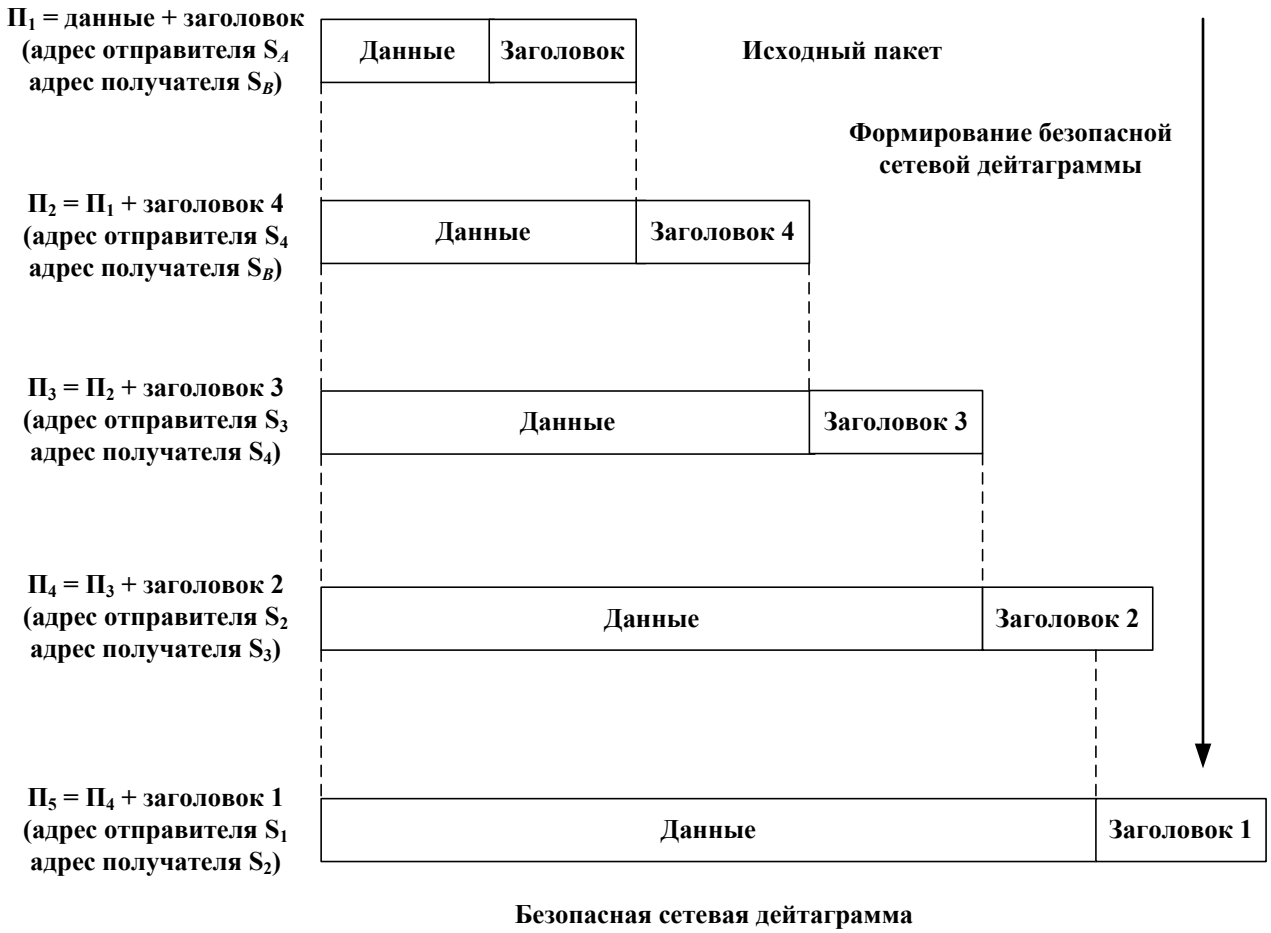


Рис. 3. Схема порядка формирования заголовка безопасной сетевой дейтаграммы

На первом этапе (блок 7 рис. 2) при формировании сетевой дейтаграммы (второй пакет – $П_2$), осуществляется шифрование информационного поля данных с использованием криптографического ключа K (блок 8 рис. 2), с указанием в заголовке адреса получателя S_B и адреса ближайшего к нему доверенного узла 2_4 отправителя, в рассматриваемом примере – S_4, в соответствии с маршрутом передачи m_1 сетевой дейтаграммы.

На втором этапе при формировании сетевой дейтаграммы (третий пакет – $П_3$) производится инкапсуляция полученной дейтаграммы ($П_2$), которая шифруется с использованием криптографического ключа K, в информационное поле новой дейтаграммы с заголовком 3, включающим адреса получателя S_4 и отправителя S_3.

На третьем этапе при формировании сетевой дейтаграммы (четвёртый пакет – $П_4$) производится инкапсуляция полученной дейтаграммы ($П_3$), которую шифруют, в информационное поле новой дейтаграммы с заголовком 2, включающим адреса получателя S_3 и отправителя S_2.

На последнем этапе (блок 9 рис. 2) при формировании сетевой дейтаграммы (пятый пакет – $П_5$) производится инкапсуляция полученной дейтаграммы (П 4), которую шифруют, в информационное поле новой дейтаграммы с заголовком 1, включающим адреса получателя S_2 и отправителя S_1. Полученная

дейтаграмма будет являться безопасной сетевой дейтаграммой D. Данные действия производятся на первом доверенном узле 2_1 (шлюз-компьютер с межсетевым экраном) на маршруте передачи исходной сетевой дейтаграммы с адресами отправителя S_A и получателя S_B.

Далее сформированная безопасная сетевая дейтаграмма D передаётся в канал связи внешней сети (блок 10 рис. 2). При получении безопасной сетевой дейтаграммы D (блок 11 рис. 2) на доверенном узле 2_2 по адресу получателя S_2, выполняется дешифрование сетевой дейтаграммы с использованием криптографического ключа K (блок 12 рис. 2). Получают дейтаграмму с адресом отправителя S_2 и адресом получателя S_3. Записывают в поле "Опции" (блок 13 рис. 2) адрес пройденного доверенного узла S_2 и передают сформированную дейтаграмму в канал связи.

Действия, производимые с безопасной сетевой дейтаграммой на маршруте её передачи, осуществляются на каждом доверенном узле (блок 14 рис. 2). На последнем узле, по маршруту продвижения дейтаграммы, будет получена сетевая дейтаграмма с адресом получателя S_B и адресом отправителя S_4. Осуществляется сравнение значений поля "опции", записанных в начале маршрута, с полученными значениями после передачи сетевой дейтаграммы (блок 15 рис. 2), в случае несовпадения маршрута принимают решение о блокировке сетевой дейтаграммы (блок 16 рис. 2).

Кроме того, для обеспечения безопасности сетевой дейтаграммы возможно использование только значений конечных адресов и определенного маршрута передачи (рис. 4), в соответствии с алгоритмом, обобщённая блок-схема которого приведена на рис. 5.

При этом может быть задано множество $M = (m_1, m_2, \ldots m_j, \ldots m_M)$ маршрутов передачи сетевых дейтаграмм (блок 3 рис. 5) по внешней сети между защищаемыми компьютерными сетями (S_A, S_B) в виде последовательности адресов доверенных узлов 2 на пути передачи сетевой дейтаграммы $m_j = (S_1, S_2, \ldots, S_r, \ldots, S_{Vj})$, где V_j – номер последнего доверенного узла 2 по j-му маршруту передачи, которые записывают в массив маршрутов M (блок 4 рис. 5).

Массив M приведён в табл. 1, в которой каждой паре абонентов соответствуют имеющиеся маршруты и их номера.

Таблица 1

Маршрутно-адресная таблица для формирования безопасной сетевой дейтаграммы

Абоненты	Номер маршрута	Маршрут
$S_A - S_B$	1	$S_A, S_1, S_2, S_3, S_4, S_B$
	2	$S_A, S_1, S_6, S_7, S_4, S_B$
	3	S_A, S_1, S_2, S_4, S_B
	4	$S_A, S_1, S_2, S_6, S_3, S_7, S_5, S_4, S_B$
	5	$S_A, S_1, S_6, S_3, S_5, S_4, S_B$
	6	$S_A, S_1, S_6, S_3, S_5, S_7, S_4, S_B$

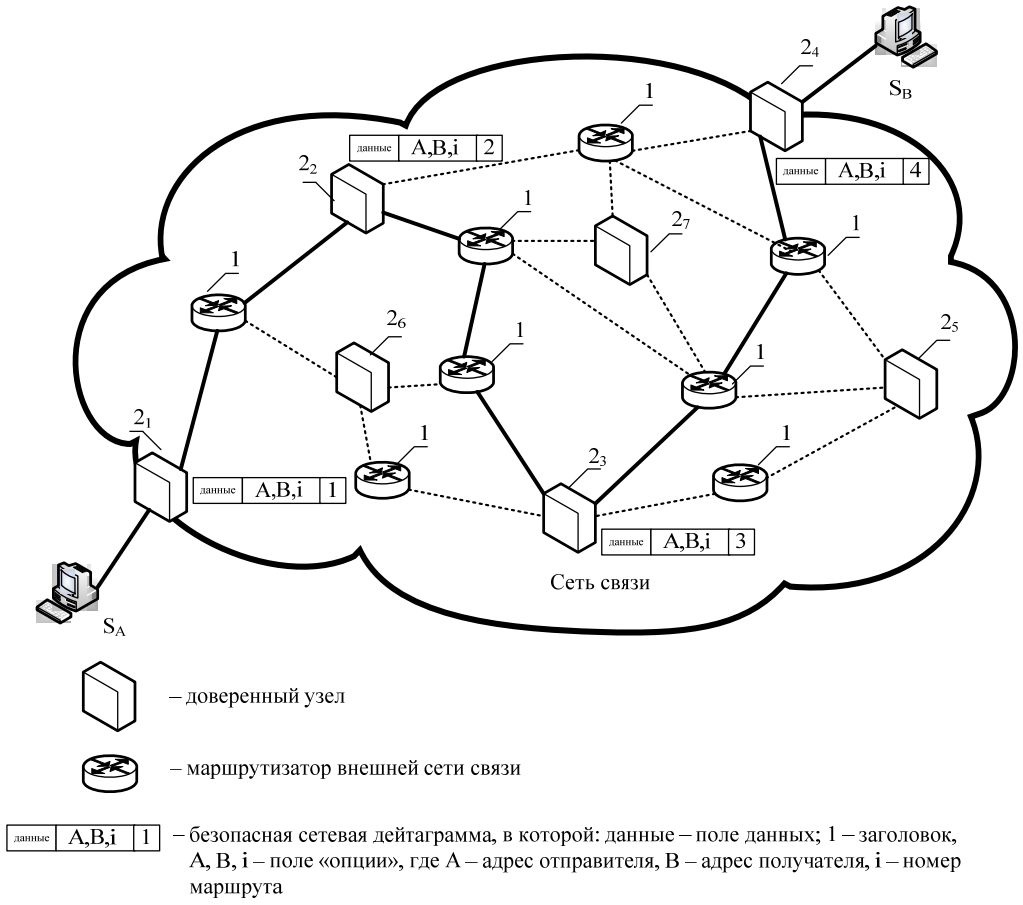
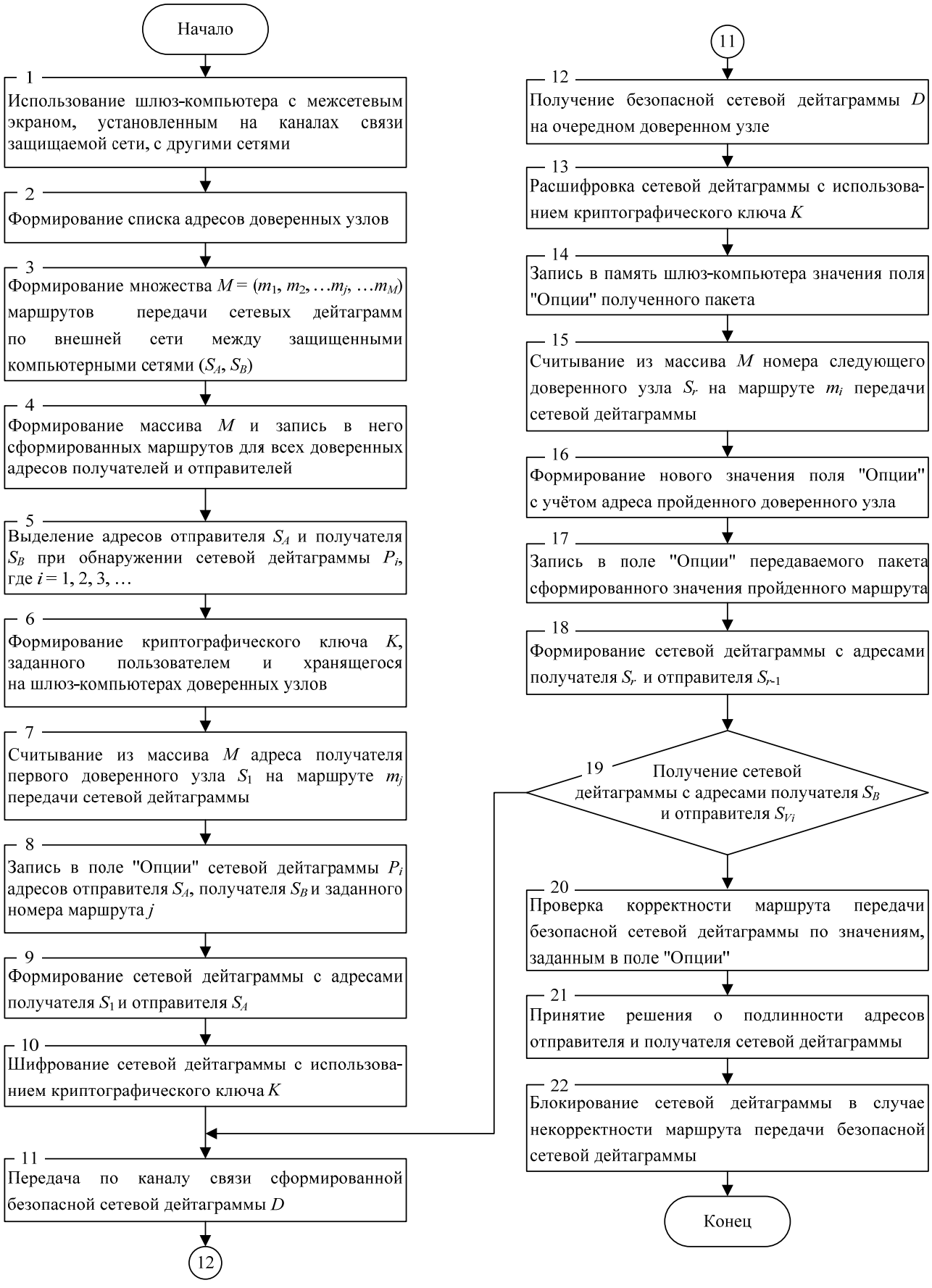


Рис. 4. Схема порядка формирования маршрута передачи пакетов сообщений в ИВС

При поступлении очередной сетевой дейтаграммы из массива M считывается номер первого доверенного узла 2_1 на маршруте m_j передачи сетевой дейтаграммы, соответствующий адресу отправителя S_A, адресу получателя S_B и заданному номеру маршрута j, который выбирается из возможных маршрутов (блок 7 рис. 5), например, по случайному закону. Кроме того, в поле "Опции" (блок 8 рис.5) сетевой дейтаграммы P_i записывается адрес отправителя S_A, адрес получателя S_B и заданный номер маршрута j.

В сформированной сетевой дейтаграмме с адресом получателя S_1 и адресом отправителя S_A шифруется информационная часть пакета с использованием криптографического ключа K (блоки 9, 10 рис.5).

При приёме безопасной сетевой дейтаграммы (блок 12 рис. 5), на каждом доверенном узле $2_{r\text{-}1}$ выполняется её дешифрование и определяется номер следующего доверенного узла 2_r на маршруте m_j передачи сетевой дейтаграммы, из массива маршрутов M (табл. 1) по соответствующим значениям адреса отправителя S_A, адреса получателя S_B и заданному номеру маршрута j, имеющимся в поле "Опции" (блок 13, 14, 15 рис. 5). После шифрования сформированной сетевой дейтаграммы, имеющей адрес получателя S_r, адрес отправителя $S_{r\text{-}1}$ и новое значение поля "Опции" с учётом адреса пройденного доверенного узла $2_{r\text{-}1}$, она передаётся в канал связи (блок 16, 17, 18 рис. 5).



#

Рис. 5. Обобщённая блок-схема алгоритма обработки дейтаграмм сетевого трафика для защиты ИВС

На последнем доверенном узле 2_{Vi} по маршруту передачи сетевой дейтаграммы (блок 19 рис.5), как и в первом варианте, осуществляется сравнение значений поля "Опции", записанных в начале маршрута, с полученными значениями после передачи сетевой дейтаграммы (блок 20 рис. 5), в случае несовпадения маршрута принимают решение о блокировке сетевой дейтаграммы (блоки 21, 22 рис. 5).

Таким образом, данный метод за счёт скрытия истинных адресов отправителя и получателя сетевых дейтаграмм путём шифрования сетевых дейтаграмм и последовательной передачи между доверенными узлами информационно-вычислительной сети в соответствии с информацией о маршруте передачи позволяет повысить достоверность обнаружения подлога компьютерных адресов отправителя и получателя сетевых дейтаграмм.

Литература

1. ***Руководящий*** документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. – М: ФСТЭК, 2008. 69 с.

2. ***Купреенко С.В., Заборовский В.С., Шеманин Ю.А.*** Вычислительна сеть с межсетевым экраном и межсетевой экран. Патент РФ № 2214623, МПК G06F 15/163, 15/173.

3. ***Shrikhande N.V.*** Application specific distributed firewall. Патент США № 6721890, МПК H04L 009/00.

4. ***Лежнев А.В., Селин Р.Н.*** Патент РФ № 2314562, МПК G06F 21/22. Опубл. 10.01.2008., бюл. № 1.

5. ***ГОСТ Р*** ИСО/МЭК 7498-1-99. Информационная технология. 1. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. М.: Издательство стандартов, 1999. 57 с.

6. ***RFC 791***, Internet Protocol, 1981, сентябрь. С. 14-22.