УДК 004.72

# АНАЛИЗ ВОЗМОЖНОСТИ БЕЗОПАСНОГО МАСШТАБИРОВАНИЯ ТЕЛЕКОММУНИКАЦИОННОЙ СТРУКТУРЫ АСУ ПУТЕМ ПРИНУДИТЕЛЬНОЙ МАРШРУТИЗАЦИИ ТРАФИКА СТАНДАРТНЫМИ СРЕДСТВАМИ

**М.В. Буйневич, А.Е. Магон, Д.М. Ширяев**

*Военно-морской институт радиоэлектроники (ВМИРЭ) имени А.С. Попова, г. Санкт-Петербург*

*Рецензент В.Е. Подольский*

**Ключевые слова и фразы:** архитектура безопасности; масштабирование; механизм управления маршрутизацией; перенаправление трафика; стандарт; телекоммуникационная структура.

**Аннотация:** Изложен подход к безопасному масштабированию телекоммуникационной структуры АСУ, детализирующий стандарт Р ИСО 7498-2–99 в части доверительной функциональности механизма управления маршрутизацией. Определена возможность принудительной маршрутизации стандартными средствами для направления трафика по определенному маршруту, проходящему через контролируемое телекоммуникационное оборудование.

В процессе своего использования любая автоматизированная система управления (**АСУ**), особенно организационного типа, постоянно эволюционирует в сторону интегрирования в процесс обработки и обмена все новых объектов информатизации, тем самым масштабируя свою телекоммуникационную структуру, в том числе, используя различные сети передачи данных. Если информация, обрабатываемая в этой интегрированной АСУ, является критичной, то ее передача между компьютерами различных сетей является небезопасной, так как существует как риск несанкционированного доступа к этой информации в процессе ее следования от отправителя к получателю, так и угроза ее целостности и доступности. Налицо необходимость в защите передаваемых данных. Практически от всех известных угроз безопасности существуют средства защиты, из которых

Буйневич М.В – кандидат технических наук, профессор ВМИРЭ, г. Санкт-Петербург; Магон А.Е. – кандидат экономических наук ВМИРЭ, г. Санкт-Петербург; Ширяев Д.М. – младший научный сотрудник научно-исследовательской лаборатории РЭВ (радиоэлектронного вооружения), г. Щелково-4.

строится современная система обеспечения безопасности информации. Однако при экстенсивном подходе функции защиты могут довести стоимость обеспечения безопасности выше возможной ценности самих данных, либо привести к такому большому времени получения данных, по истечении которого ценность этих данных снижается (или теряется). Нужна рациональная архитектура безопасности телекоммуникационной структуры интегрированной АСУ.

ГОСТ Р ИСО 7498-2–99 [1] определяет общие архитектурные элементы защиты данных, передаваемых между системами класса «интегрированная АСУ», дополняя в части безопасности базовую эталонную модель взаимодействия открытых систем (**ЭМ ВОС**). Этот документ содержит общее описание услуг и соответствующих механизмов защиты, которые могут быть обеспечены эталонной моделью, а также определяет те позиции в рамках эталонной модели, в которых могут обеспечиваться эти услуги и механизмы.

Рассмотрим механизм управления маршрутизацией, изложенный в п. 5.3.7.1 ГОСТ, с позиции реализации доверительной функциональности стандартными средствами. Этот механизм используется на сетевом уровне ЭМ ВОС для ограничения путей, по которым передаются данные от одного автоматизированного рабочего места (**АРМ**), – «отправителя», к другому АРМ – «получателю». Выбор маршрутов может управляться пользовательскими системами или выполняться на промежуточных системах. Этот механизм может быть также использован для поддержки средства целостности с восстановлением, например, выбирая альтернативные пути после атак, повредивших пути взаимодействия. В любом случае этот механизм явно требует доверия к промежуточным системам, под которыми понимается контролируемое телекоммуникационное оборудование, исключающее возможность подмены, модификации или внедрения информации в потоки данных, проходящих через них.

Для определения возможности принудительной маршрутизации для направления трафика по определенному маршруту, проходящему через контролируемое телекоммуникационное оборудование, рассмотрим схему фрагмента сети.

Схема реализует следующую концепцию передачи информации:

– обмен информацией производится между АРМ2 и АРМ1;

– маршрутизаторы Router1, Router3, Router4, Router5 являются контролируемыми;

– маршрутизатор Router2 является неконтролируемым;

– в результате трассировки информационных потоков выявлено, что маршрут передачи информации проходит через маршрутизаторы Router5, Router2, Router1, то есть выходит за пределы контролируемой зоны.

Для перенаправления трафика в пределах контролируемой зоны могут быть предложены следующие методы: метод использования статических маршрутов и метод использования параметров IP-опций «жесткая маршрутизация».

Метод использования статических маршрутов предназначен для перенаправления трафика в контролируемый сегмент сети и основан на вне-

сении изменений в текущую конфигурацию маршутизаторов [3], определяющих IP-адрес следующего маршрутизатора для передачи трафика до сети получателя информации.

Алгоритм метода использования статических маршрутов для перенаправления трафика в контролируемый сегмент сети следующий:

1) определяются IP-адреса неконтролируемого и предыдущего контролируемого маршрутизаторов по результатам анализа маршрута передачи трафика;

2) осуществляется подключение к контролируемому маршрутизатору на привилегированном уровне;

3) в конфигурационный файл маршрутизатора добавляется строка, содержащая информацию о статическом маршруте;

4) проводится анализ измененного маршрута для оценки достижимости сети получателя информации.

Анализ маршрута следования пакета показал, что он изменился и проходит только в переделах контролируемой зоны.

Ограничением метода является следующее:

– требуется получение полного доступа к маршрутизатору;

– при использовании статической маршрутизации маршрутизатор не может обнаружить отказ транзитного маршрутизатора, поэтому выход из строя транзитного маршрутизатора приведет к разрыву канала передачи данных.

Метод перенаправления трафика с помощью параметров опции IP-пакета основан на использовании типа параметра 0×89 для жесткой маршрутизации поля опции IP-пакета.

Жесткая маршрутизация от источника. В данной опции отправитель точно фиксирует весь путь следования IP-дейтаграммы. Если маршрутизатор обнаруживает, что согласно жестко заданному маршруту он должен переправить дейтаграмму на узел, с которым не связан по сети напрямую (в пределах одного физического сегмента), то он удаляет пакет и отправляет на исходный хост ICMP-сообщение об ошибке.

Алгоритм метода перенаправления трафика с использованием «жесткой маршрутизации» от источника следующий:

1) определяются IP-адреса неконтролируемого и последнего контролируемого маршрутизаторов по результатам анализа передачи трафика;

2) определяется IP-адрес контролируемого маршрутизатора, являющегося соседним с последним контролируемым в текущем маршруте;

3) в поле опций IP-пакета последовательно заносятся адреса: соседнего маршрутизатора, всех транзитных маршрутизаторов до получателя информации, адрес конечного получателя информации;

4) в поле «адрес получателя» заголовка IP-пакета записывается адрес последнего контролируемого маршрутизатора;

5) проводится анализ измененного маршрута для оценки достижимости сети получателя информации.

Ограничением метода является следующее:

– на маршрутизаторе должна быть разрешена маршрутизация от источника, то есть в конфигурационном файле отсутствует строка *no ip source*;

– количество записанных IP-адресов ограничено размером поля «данные» параметра.

Несмотря на выявленные ограничения, достоинства вышерассмотренных методов, а именно: возможность реализации стандартными методами, быстрота реализации и достоверность полученной информации,– позволяют сделать вывод о реализации определенной доверительной функциональности стандартных алгоритмов управления маршрутизацией и, как следствие, о возможности безопасного масштабирования телекоммуникационной структуры АСУ путем принудительной маршрутизации трафика стандартными средствами.

*Список литературы*

1. ГОСТ Р ИСО 7498-2-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации. – Введ. 01-01-2000. – М. : Изд-во стандартов, 1999. – 39 с.

2. Семенов, Ю.А. Протоколы Internet. Энциклопедия / Ю.А. Семенов. – М. : Изд-во: «Горячая линия-Телеком, Радио и связь», 2001. – 1100 с.

3. Леинванд, А. Конфигурирование маршрутизаторов Cisco / А. Леинванд, Б. Пински. – М. : Вильямс, 2004. – 368 с.

---

**Analysis of the Possibility of Secure Auto-Dimensioning of Telecommunication Structure of CAD via Assisted Routing of Traffic by Standard Means**

**M.V. Buinevich, A.E. Magon, D.M. Shiryaev**

*Military Navy Institute of Radio Electronics named after A.S. Popov, St. Petersburg*

**Key words and phrases:** security architecture; auto-dimensioning; routing control mechanism; traffic redirection; standard; telecommunication structure.

**Abstract:** The paper presents the approach to secure auto-dimensioning of telecommunication structure of CAD; it gives the details of standard P ISO 7408-2–99 with regard for confidential functionality of the routing control mechanism. The possibility of assisted routing by standard means of traffic direction in the given route running through the controlled telecommunication equipment is revealed.

---