СПОСОБ ЗАЩИТЫ ОТ ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ В МУЛЬТИСЕРВИСНЫХ СЕТЯХ СВЯЗИ

Бухарин В.В.[1], Карайчев С.Ю.[2], Пикалов Е.Д.[3]

В статье рассматриваются вопросы, касающиеся построения систем защиты для обеспечения информационной безопасности при реализации деструктивных программных воздействий. При этом отмечается, что указанные системы защиты используются в мультисервисных сетях связи, характеризующихся наличием в них сетевых элементов, обладающих широкими возможностями удаленного управления. Указывается, что данные сетевые элементы являются основой транспортной сети с коммутацией пакетов и реализация деструктивных программных воздействий на них приводит к блокированию доступа к информационным ресурсам мультисервисной сети связи, что связано с отсутствием необходимых маршрутов передачи сообщений. Подробно описывается последовательность действий, поясняющая сущность предложенного способа защиты от деструктивных программных воздействий. В статье показано, что рассмотренный способ обеспечивает повышение защищенности мультисервисной сети связи за счет определения маршрутов передачи пакетов сообщений, на которых имеются сетевые элементы, подверженные деструктивным программным воздействиям, и, соответственно, исключение повторного использования данных маршрутов. Делается вывод о том, что разработанный способ защиты в качестве положительного эффекта предполагает уменьшение времени обнаружения деструктивных программных воздействий при увеличении количества сетевых элементов мультисервисных сетей связи в сравнении с известным способом защиты.

***Ключевые слова**: информационная безопасность, система защиты, сетевые элементы, удаленное управление, маршрут, пакеты сообщений, информационные ресурсы.*

Введение

На современном этапе развития информационной безопасности широкое распространение получили системы защиты от различных деструктивных программных воздействий (ДПВ). При этом существующие системы защиты, в том числе используемые на мультисервисных сетях связи (МСС), ориентированы на ДПВ, направленные на абонентские терминалы или сетевые сервисные узлы, а также другие оконечные сетевые средства [1, 2]. Однако фактически все сетевые элементы, составляющие транспортную основу МСС, имеют возможности удаленного мониторинга, конфигурирования и управления через различные открытые интерфейсы [3]. Таким образом, имеется возможность реализации ДПВ на данных элементах, что приводит к существенным потерям пропускных способностей МСС и даже блокированию доступа к информационным ресурсам при отсутствии необходимого маршрута передачи или несоответствии скорости передачи сообщений по имеющему маршруту.

Существующие способы, реализуемые в системах защиты, имеют относительно низкую защищенность от ДПВ, обусловленную выполнением соответствующих действий по обнаружению ДПВ для пакетов сообщений, переданных только по одному маршруту в МСС [4, 5], а также значительное увеличение времени обнаружения ДПВ при увеличении количества сетевых элементов МСС.

Постановка задачи

Задачей исследования являлась разработка способа защиты от ДПВ в МСС, обеспечивающего расширение функциональных возможностей существующих способов по повышению защищенности от ДПВ за счет определения маршрутов передачи пакетов сообщений, на которых имеются узлы, подверженные ДПВ, и, соответственно, исключение повторного использования данных маршрутов, а также при увеличении количества сетевых элементов МСС уменьшение времени на обнаружение ДПВ.

1 Бухарин Владимир Владимирович, доктор технических наук, Академия ФСО России, г. Орёл, bobah_buch@mail.ru
2 Карайчев Сергей Юрьевич, Академия ФСО России, г. Орёл, serg_mts@inbox.ru
3 Пикалов Евгений Дмитриевич, кандидат технических наук, Академия ФСО России, г. Орёл, evgenii-78@yandex.ru

Сущность способа защиты от деструктивных программных воздействий в мультисервисных сетях связи

Реализация разработанного способа поясняется блок-схемой последовательности действий (рис. 1), схемой (рис. 2) и объясняется следующим образом:

На начальном этапе формируют массивы P, D, I, T, $D_{эт}$, $I_{эт}$, $T_{исх}$, $T_{эт}$ для запоминания параметров, задаваемых и выделенных из запомненных пакетов сообщений соответственно (блок 1, рис. 1):

P – для запоминания поступающих из канала связи IP-пакетов сообщений;

D – для запоминания значений поля данных «IP-адрес назначения»;

I – для запоминания значений поля данных «IP-адрес источника»;

T – для запоминания значений поля данных «Время жизни пакета»;

$D_{эт}$ – для запоминания эталонных параметров значений поля данных «IP-адрес назначения»;

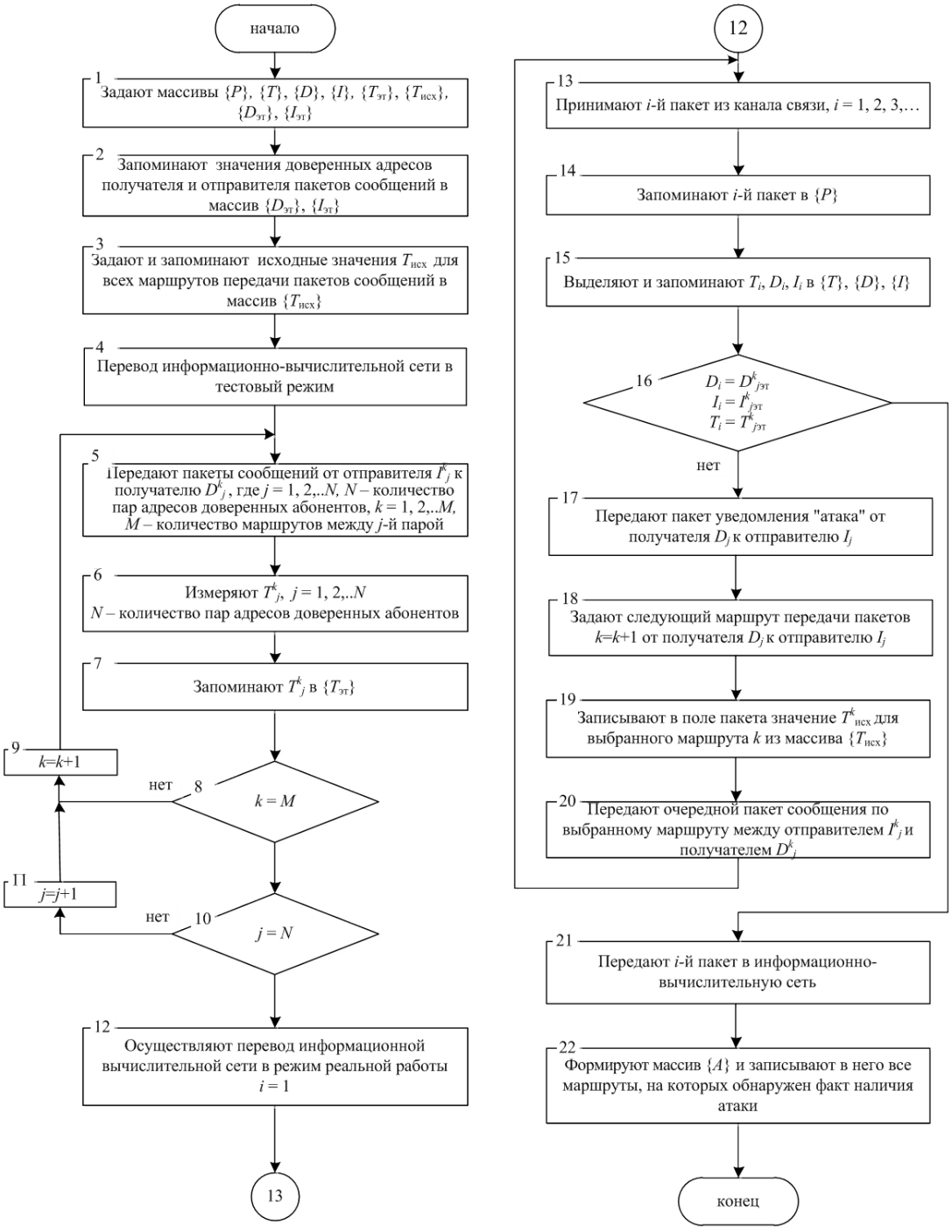

***Рис. 1**. Блок-схема последовательности действий способа защиты МСС от ДПВ*

$I_{эт}$ – для запоминания эталонных параметров значений поля данных «IP-адрес источника»;

$T_{исх}$ – для запоминания исходных параметров значений поля данных «Время жизни пакета»;

$T_{эт}$ – для запоминания эталонных параметров значений поля данных «Время жизни пакета».

В предлагаемом способе используют функции IP-протокола, применяемые при передаче пакетов по сети. Заголовок протокола IP содержит множество полей, в том числе поля «IP-адрес назначения» и «IP-адрес источника», в которых будут находиться 32 битные последовательности, определяющие логические адреса назначения и источника пакета сообщения, необходимые для передачи его по МСС. Поле «Время жизни пакета» определяет максимальное время существования дейтаграммы в сети [6].

Далее определяют доверенные IP-адреса получателя и отправителя для запоминания этих значений в массив $D_{эт}$, $I_{эт}$ (блок 2, рис.1). Под доверенными IP-адресами понимают пары адресов источника и назначения легитимных абонентов различных фрагментов МСС и запоминают данные значения доверенных адресов получателя и отправителя пакетов сообщений в соответствующих массивах.

Кроме того, задаются и запоминаются исходные значения $T_{исх}$ параметров поля данных «Время жизни пакета» для всех маршрутов передачи пакетов сообщений (блок 3, рис. 1), при этом данные значения задаются с учетом количества узлов сети связи на маршруте передачи.

Таким образом, последовательность узлов, лежащих на пути от отправителя к получателю, образует маршрут передачи сообщений [7].

Это связано с тем, что значение поля «Время жизни пакета» необходимо для реализации механизма стирания пакетов, у которых значение данного поля равно нулю [6]. Для обеспечения гарантированной доставки пакетов до получателя значение данного поля должно превышать количество промежуточных узлов на маршруте передачи. В общем случае исходное значение $T_{исх}$ параметра поля данных «Время жизни пакета» может быть выбрано одинаковым для всех маршрутов, но оно должно соответствовать наиболее протяженному маршруту, имеющему большее количество узлов. Например, на рисунке 2 показано пять возможных маршрутов передачи пакетов по

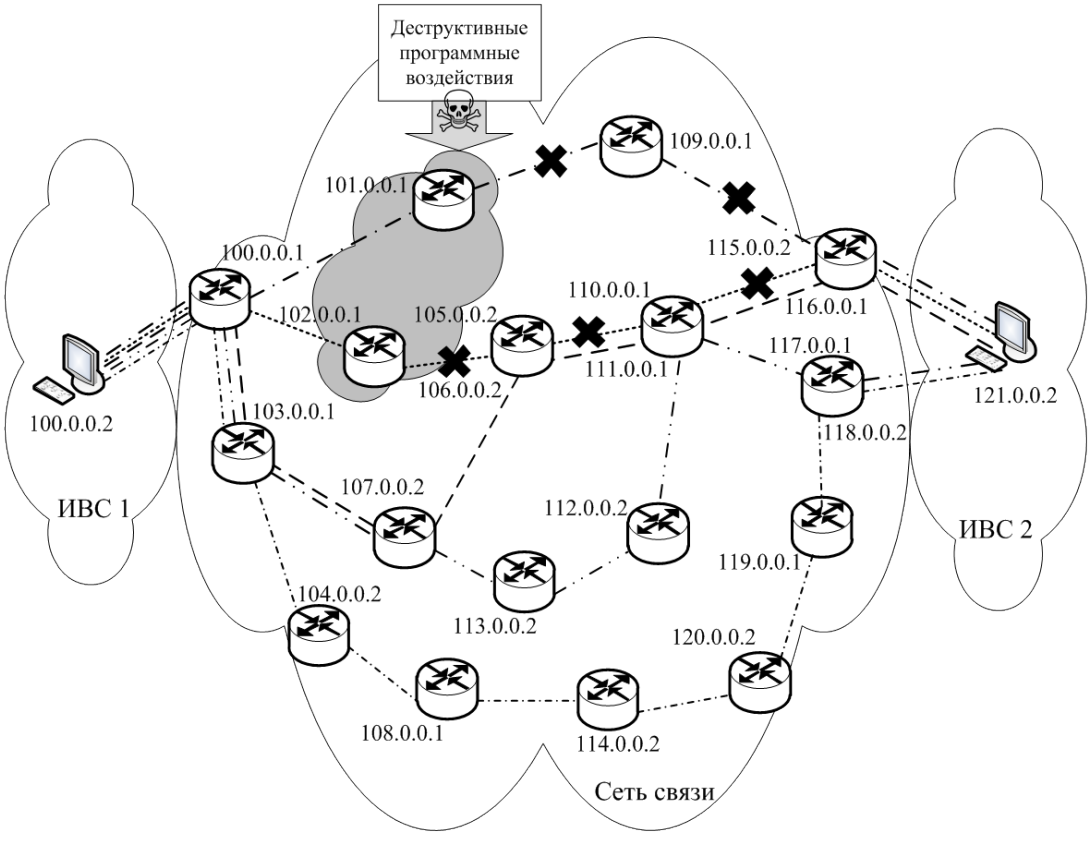

Рис. 2. *Схема, поясняющая реализацию ДПВ и изменение маршрутов передачи пакетов сообщений в МСС*

Таблица 1

Эталонные и исходные значения полей данных «IP-адрес назначения», «IP-адрес источника» и «Время жизни пакета» для определенных маршрутов

Номер маршрута	IP-адрес источника	IP-адрес назначения	Исходные значения $T_{исх}$	Эталонные значения $T_{эт}$	Маршрут
1	100.0.0.2	121.0.0.2	10	6	100.0.0.1; 101.0.0.1; 109.0.0.1; 115.0.0.2
2			10	5	100.0.0.1; 102.0.0.1; 105.0.0.2; 110.0.0.1; 115.0.0.2
3			10	4	100.0.0.1; 103.0.0.1; 107.0.0.2; 106.0.0.2; 110.0.0.1; 115.0.0.2
4			10	3	100.0.0.1; 103.0.0.1; 107.0.0.2; 113.0.0.2; 112.0.0.2; 111.0.0.1; 117.0.0.1
5			10	2	100.0.0.1; 103.0.0.1; 104.0.0.2; 108.0.0.1; 114.0.0.2; 120.0.0.2; 119.0.0.1; 118.0.0.2

сети связи между отправителем и получателем. Так, для первого маршрута, состоящего из промежуточных узлов с адресами 100.0.0.1; 101.0.0.1; 109.0.0.1; 115.0.0.2 достаточным значением поля данных «Время жизни пакета» является пять, а для пятого маршрута, состоящего из промежуточных узлов с адресами 100.0.0.1; 103.0.0.1; 104.0.0.2; 108.0.0.1; 114.0.0.2; 120.0.0.2; 119.0.0.1; 118.0.0.2 достаточным значением поля данных «Время жизни пакета» является уже девять.

Учитывая, что пятый маршрут имеет максимальное количество промежуточных узлов, то $T_{исх}$ может быть выбрано равным десяти для всех маршрутов (табл. 1).

Затем осуществляется перевод МСС в тестовый режим функционирования, который подразумевает ее адаптацию к реальным условиям (блок 4, рис.1). Под адаптацией в соответствии с [8] понимается работа информационно-вычислительной сети в тестовом режиме для внедрения ее в конкретные условия функционирования. При этом в тестовом режиме предполагаются идеальные условия функционирования сети связи, т. е. отсутствие ДПВ, что позволяет получить эталонные значения необходимых характеристик передаваемых пакетов сообщений. В данном режиме осуществляется передача пакетов сообщений между всеми парами от отправителя I^k_j к получателю D^k_j, $j = 1, 2,\ldots N$, где N – количество пар адресов доверенных абонентов по всем имеющимся маршрутам $k = 1, 2,\ldots M$, где M – количество маршрутов между j-й парой адресов доверенных абонентов (блок 5, рис.1).

Далее у получателя измеряют реальные значения поля данных пакета «Время жизни пакета» T^k_j для всех имеющихся маршрутов $k = 1, 2,\ldots M$ для всех существующих пар адресов доверенных абонентов $j = 1, 2,\ldots N$ (блоки 6–11, рис.1).

При передаче пакетов по сети промежуточные узлы (маршрутизаторы) осуществляют их маршрутизацию по адресной информации, имеющейся в заголовке пакета [9]. Таким образом, полученные значения поля данных пакета «Время жизни пакета» T^k_j показывают количество промежуточных узлов, через которые передан пакет сообщения по k-му маршруту между j-й парой отправитель–получатель.

Например, для маршрутов передачи пакетов сообщения (рис. 2) приведены измеренные значения поля данных пакета «Время жизни пакета» Tkj (табл. 1), которые являются эталонными (так как они получены в тестовом режиме функционирования) для соответствующих маршрутов и будут записаны в массив $\{T_{эт}\}$ (блок 7, рис. 1). Так, для первого маршрута, учитывая заранее заданное у отправителя исходное значение параметра поля данных «Время жизни пакета» $T_{исх}$=10, на каждом промежуточном узле (маршрутизаторе),

через которые передается пакет сообщения (узлы: 100.0.0.1; 101.0.0.1; 109.0.0.1; 115.0.0.2), значение поля данных «Время жизни пакета» уменьшается на единицу [4] и эталонное значение поля данных «Время жизни пакета» принятого пакета у получателя получится равным $T_{эт}$ = 10 – 4 = 6. Аналогично для маршрутов 2–5 (рис. 2) приведены соответствующие эталонные значения поля данных «Время жизни пакета» (табл. 1): маршрут 2 имеет пять промежуточных узлов (100.0.0.1; 102.0.0.1; 105.0.0.2; 110.0.0.1; 115.0.0.2) и эталонные значения $T_{эт}$ = 10 – 5 = 5; маршрут 3 имеет шесть промежуточных узлов (100.0.0.1; 103.0.0.1; 107.0.0.2; 106.0.0.2; 110.0.0.1; 115.0.0.2) и эталонные значения $T_{эт}$ = 10 – 6 = 4; маршрут 4 имеет семь промежуточных узлов (100.0.0.1; 103.0.0.1; 107.0.0.2; 113.0.0.2; 112.0.0.2; 111.0.0.1; 117.0.0.1) и эталонные значения $T_{эт}$ = 10 – 7 = 3; маршрут 5 имеет восемь промежуточных узлов (100.0.0.1; 103.0.0.1; 104.0.0.2; 108.0.0.1; 114.0.0.2; 120.0.0.2; 119.0.0.1; 118.0.0.2) и эталонные значения $T_{эт}$ = 10 – 8 = 2.

После того как все эталонные значения проверяемых параметров собраны и записаны в соответствующие массивы, осуществляют перевод МСС в режим реальной работы (эксплуатация) (блок 12, рис.1), при этом на МСС злоумышленники будут осуществлять различные воздействия, в том числе реализуя ДПВ.

Далее при функционировании МСС получатель принимает i-й пакет сообщения из канала связи, запоминает его в массиве P для дальнейшей работы с заголовком i-го пакета (блоки 13, 14, рис.1). После этого выделяют из заголовка i-го пакета значения поля данных «Время жизни пакета» T_i, поля данных «IP-адрес назначения» D_i и поля данных «IP-адрес источника» I_i и запоминают их в массивах $\{T\}$, $\{D\}$, $\{I\}$.

Затем производится сравнение запомненных значений D_i, I_i принятого пакета сообщения с эталонными значениями из массивов $\{D_{эт}\}$, $\{I_{эт}\}$, определение пары отправитель–получатель (конкретная j-я пара доверенных абонентов) и определение соответствующего маршрута передачи данного пакета сообщения при сравнении запомненного значения T_i с эталонными значениями из массива $\{T_{эт}\}$ для данной пары отправитель–получатель (блок 16, рис.1). При этом если ДПВ оказывает влияние на узлы 101.0.0.1 и 102.0.0.1 (рис. 2), то первый и второй маршруты (табл. 1) будут недоступны для передачи пакетов сообщений, так как данные узлы входят в соответствующие маршруты (узел 101.0.0.1 – в первый маршрут, узел 102.0.0.1 – во второй маршрут). В этом случае узел 100.0.0.1, работающий как маршрутизатор, имеет в таблице маршрутизации несколько (для приведенного примера пять) альтернативных маршрутов [7]. Из них выбирается определенный маршрут по заданному критерию, например задержка прохождения маршрута пакетом [7], т. е. количество промежуточных узлов на маршруте. Таким образом, маршрутизатор выберет третий маршрут, имеющий по данному критерию превосходство над остальными (меньшее количество промежуточных узлов), который является альтернативным относительно первого и второго маршрутов.

В случае невыполнения условия (блок 16, рис.1) от получателя D_j к отправителю I_j передается пакет, уведомляющий об «установлении факта наличия ДПВ» (блок 17, рис. 1) и отправитель задает следующий маршрут передачи пакетов $k = k + 1$ для данной пары отправитель–получатель (для приведенного примера выбирается третий маршрут) (табл. 1), а для него выбирается и записывается в поле данных «Время жизни пакета» соответствующее исходное значение из массива $\{T_{исх}\}$ (блок 19, рис.1).

Затем по выбранному маршруту передается очередной пакет сообщения (блок 20, рис.1) от отправителя к получателю и для данного пакета повторно осуществляются действия, начиная с приема пакета сообщения из канала связи (блок 13, рис.1). В случае если условия (блок 16, рис.1) выполняются, то делается вывод об отсутствии факта ДПВ и передают данный i-й пакет сообщения в информационно-вычислительную сеть (блок 21, рис.1).

В заключение формируется массив $\{A\}$, и в него записываются все маршруты, для которых установлен факта наличия ДПВ (блок 22, рис. 1), что позволяет исключить повторное их использование для передачи пакетов сообщения.

Выводы

Возможность реализации сформулированного в способе решения была проверена путем машинного моделирования, с помощью которого получена взаимосвязь значений времени распознавания $t_{обн}$ (обнаружения) ДПВ от количества узлов сети связи N (рис. 3).

Достижение технического результата поясняется следующим образом. Для известного способа при обнаружении ДПВ [10] осуществляется сравнение значений полей данных «Время жизни пакета» и «Опции» пакетов за время T_1, которое

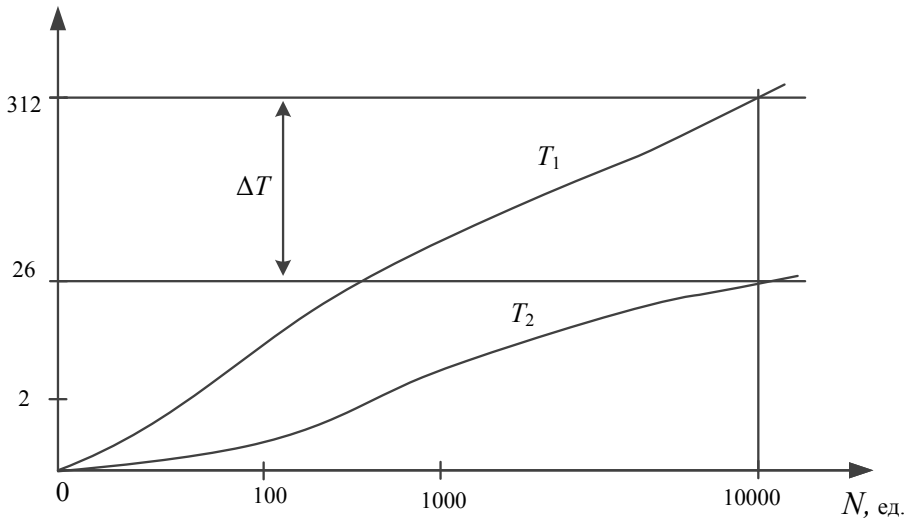

***Рис. 3**. Зависимость времени обнаружения ДПВ от количества сетевых элементов МСС*

зависит в основном от значений поля «Опции», так как в нем размещается маршрут передачи пакета – это 3–15 узлов в маршруте [7], а он состоит из адресов промежуточных узлов – это 4 байта в десятичной форме 12 разрядов [7]. Для предлагаемого способа выявление ДПВ производится по результатам анализа значений поля данных «Время жизни пакета» принятого пакета за время T_2, которые зависят только от количества узлов в маршруте передачи – это 2–3-разрядное число в десятичной форме. При этом разница в требуемом времени для обнаружения ДПВ $\Delta T = T_1 - T_2$ тем больше, чем больше количество сетевых элементов, этим и достигается предполагаемый эффект разработанного способа.

Кроме того, защищенность от ДПВ для приведенного примера повышается так как из имеющихся пяти маршрутов передачи пакетов сообщений в двух имеются узлы, подверженные ДПВ, и в предлагаемом способе по ним исключена повторная передача пакетов сообщения. В этом случае защищенность МСС от ДПВ повышается на 25 %.

Таким образом, разработанный способ за счет определения маршрутов передачи пакетов сообщений, на которых имеются узлы, подверженные ДПВ, и, соответственно, исключения повторного использования данных маршрутов позволяет повысить защищенность МСС от ДПВ, а также при увеличении количества сетевых элементов уменьшить время на их обнаружение.

***Рецензент**: Хахамов Павел Юрьевич, доктор военных наук, доцент, сотрудник Академии ФСО России, h7p2@rambler.ru*

Литература:

1. Гречишников Е.В., Горелик С.П., Добрышин М.М. Способ обеспечения требуемой защищенности сети связи от внешних деструктивных воздействий // Телекоммуникации. 2015. № 6. С. 32-37.
2. Гречишников Е.В., Добрышин М.М. Оценка эффективности деструктивных программных воздействий на сети связи // Системы управления, связи и безопасности. 2015. № 2. С. 135-146.
3. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH – СПб.: БХВ-Петербург, 2006. 366 с.
4. Ерёменко, В.Т., Батенков А.А., Полянский И.С., Батенков К.А., Сазонов М.А. Синтез локально-оптимальной структуры классификатора информационных ресурсов по критерию минимума средней длины процедуры поиска // Вестник компьютерных и информационных технологий. 2013. № 7 (109). С. 3-8.
5. Ерёменко В.Т., Парамохин В.М. Метод формирования тестовых комплектов для протоколов безопасности в системах обработки данных // Информационные системы и технологии. 2015. № 2 (88). С. 131-137.
6. Jon Postel. Internet Protocol. RFC 791 (Standard). 1981, pp. 14–22.
7. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы (5-е изд.). – СПб.: Питер, 2016. 992 с.
8. ГОСТ Р 53622–2009 «Информационные технологии. Информационно-вычислительные системы. Стадии и этапы жизненного цикла, виды и комплектность документов», с. 4–5.
9. ГОСТ Р ИСО/МЭК 7498-1–1999 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 1. Базовая модель», с.13.
10. Бухарин В. В., Дворядкин В. В. и др. / Способ защиты информационно-вычислительных сетей от компьютерных атак / Патент на изобретение № 2472211 от 10.01.2013.

PROTECTION METHOD FROM DESTRUCTIVE SOFTWARE EFFECTS IN MULTISERVICE NETWORKS

Buharin V.V.[4], Karaichev S.Yu.[5], Pikalov E.D.[6]

The article deals with the protection systems construction ensuring information security under destructive software effects. These protection systems are noted to be used in multiservice communication networks characterized by the presence of network elements capable of remote control. These network elements are considered to be the backbone of the packet switching transport network and the destructive software effects their implementation in it, in this case it can lead to the information resources access blocking of the multiservice communication network because of a lack of necessary communication routes. The operation sequence for explaining the essence of the proposed protection method from destructive software effects are described in detail. The considered method ensures the improved protection multi–service communication network by determining message packets transmission routes which are network elements affected by the destructive software effects, hence there is an exclusion of repeated data routes. In the conclusion it is necessary to note that the developed protection method provides the detection time reduction of destructive software effects at increasing the network elements number of multi–service communication network in comparing with the well–known protection method.

***Keywords**: information security, security system, network elements, remote management, route, message packets, information resources.*

References:

1. Grechishnikov E.V., Gorelik S.P., Dobryshin M.M. Sposob obespecheniya trebuemoy zashchishchennosti seti svyazi ot vneshnikh destruktivnykh vozdeystviy, Telekommunikatsii. 2015. No 6, pp. 32-37.
2. Grechishnikov E.V., Dobryshin M.M. Otsenka effektivnosti destruktivnykh programmnykh vozdeystviy na seti svyazi, Sistemy upravleniya, svyazi i bezopasnosti. 2015. No 2, pp. 135-146.
3. Gol'dshteyn A.B., Gol'dshteyn B.S. SOFTSWITCH – SPb.: BKhV-Peterburg, 2006. 366 P.
4. Eremenko, V.T., Batenkov A.A., Polyanskiy I.S., Batenkov K.A., Sazonov M.A. Sintez lokal'no-optimal'noy struktury klassifikatora informatsionnykh resursov po kriteriyu minimuma sredney dliny protsedury poiska, Vestnik komp'yuternykh i informatsionnykh tekhnologiy. 2013. No 7 (109), pp. 3-8.
5. Eremenko V.T., Paramokhin V.M. Metod formirovaniya testovykh komplektov dlya protokolov bezopasnosti v sistemakh obrabotki dannykh, Informatsionnye sistemy i tekhnologii. 2015. No 2 (88), pp. 131-137.
6. Jon Postel. Internet Protocol. — RFC 791 (Standard). — 1981, pp. 14–22.
7. Olifer V.G., Olifer N.A. Komp'yuternye seti. Printsipy, tekhnologii, protokoly (5-e izdanie). – SPb.: Piter, 2016. 992 P.
8. GOST R 53622–2009 «Informatsionnye tekhnologii. Informatsionno-vychislitel'nye sistemy. Stadii i etapy zhiznennogo tsikla, vidy i komplektnost' dokumentov», pp. 4–5.
9. GOST R ISO/MEK 7498-1–1999 «Informatsionnaya tekhnologiya. Vzaimosvyaz' otkrytykh sistem. Bazovaya etalonnaya model'. Ch. 1. Bazovaya model'», p.13.
10. Bukharin V. V., Dvoryadkin V. V. i dr., Sposob zashchity informatsionno-vychislitel'nykh setey ot komp'yuternykh atak, Patent na izobretenie No 2472211 ot 10.01.2013.

4 Vladimir Buharin, Dr.Sc., The Academy of Federal Security Guard Service of the Russian Federation, Orel, bobah_buch@mail.ru
5 Sergey Karaichev, The Academy of Federal Security Guard Service of the Russian Federation, Orel, serg_mts@inbox.ru
6 Evgeniy Pikalov, Ph.D., The Academy of Federal Security Guard Service of the Russian Federation, Orel, evgenii-78@yandex.ru