УДК 004.7

Ю.И. Стародубцев, А.Г. Чукариков, А.С. Корсунский, В.Г. Федоров

СПОСОБ ЗАЩИТЫ ИНФОТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ОТ СЕТЕВЫХ КОМПЬЮТЕРНЫХ АТАК

Стародубцев Юрий Иванович, *доктор военных наук, профессор, окончил Кемеровское высшее военное командное училище связи, Военную академию связи им. С.М. Буденного. Заслуженный деятель науки РФ, академик Российской Академии военных наук, Академии безопасности и правопорядка, Российской Академии естественных наук, Арктической академии, почетный работник высшего профессионального образования. Профессор ВАС. Имеет монографии, учебные пособия, статьи и изобретения в области защиты информационного ресурса систем военной связи и АСУ в условиях информационной войны. [e-mail: vas@mail.ru].*

Чукариков Александр Геннадьевич, *кандидат военных наук, доцент, окончил Ульяновское командное училище связи, ВАС. Доцент ВАС. Имеет статьи, монографии, изобретения в области радиоэлектронной защиты, организации и контроля безопасности связи и защиты информации. [e-mail: agchuk@yandex.ru].*

Корсунский Андрей Сергеевич, *кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру ВАС им. С.М. Буденного. Главный специалист ФНПЦ АО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации, а также передачи информации по беспроводным каналам связи информационно-телекоммуникационных систем. [e-mail: aksspb@mail.ru].*

Федоров Вадим Геннадиевич, *окончил Новочеркасское высшее военное командное училище связи. Адъюнкт ВАС им. С.М. Буденного. Имеет статьи и изобретения в области информационной безопасности. [e-mail: Vadim.fedorov.53@mail.ru].*

Аннотация

В статье рассмотрена проблема обеспечения безопасности и защиты информации в инфотелекоммуникационных сетях. Известно, что для обеспечения информационной безопасности необходимо с высокой вероятностью определять факты сетевых компьютерных атак. Имеется большое количество систем и способов обнаружения деструктивных программных воздействий на защищаемую сеть. Однако существующие технические решения не позволяют достичь необходимой вероятности обнаружения и распознавания типа деструктивных программных воздействий, имеющих своей целью формирование трафика сложной структуры. В статье предложен способ защиты инфотелекоммуникационных сетей от воздействия деструктивного трафика сложной структуры посредством введения нового отличительного признака для определения этого класса сетевых компьютерных атак и фиксирования его во времени. В способе обеспечивается адаптивная коррекция установленных правил разграничения доступа с учетом реальных характеристик обслуживаемого трафика для сохранения вероятностно-временных характеристик качества обслуживания абонентов без увеличения производительности вычислительных ресурсов на узле связи.

Ключевые слова: критически важные объекты, защищенность инфотелекоммуникационных сетей, защита от сетевых компьютерных атак, деструктивный трафик сложной структуры.

A METHOD FOR PROTECTING THE INFORMATION-TELECOMMUNICATION NETWORKS AT OBJECTS BEING OF CRITICAL IMPORTANCE AGAINST COMPUTER NETWORK ATTACKS

Iurii Ivanovich Starodubtsev, *Doctor of Military Sciences, Professor; graduated from the Kemerov Military Academy of Communications, the Marshal Budjonny Military Academy of Signal Corps; Honored Worker of Science of the Russian Federation, Academician of the Russian Academy of Military Sciences, Security Forces Academy, Russian Academy of Natural Sciences, Arctic Academy of Sciences; Honored Worker of Higher Professional Education, Professor of Military Communications Academy; an author of monographs, manuals, articles, and inventions*

in the field of information-resources security of military communication systems and computer-aided control systems in infowar contexts. e-mail: vas@mail.ru.

Aleksandr Gennadievich Chukarikov, *Candidate of Military Sciences, Associate Professor; graduated from the Ulyanovsk Military Academy of Communications; Associate Professor of the Military Academy of Communications; an author of articles, monographs, and inventions in the field electronic protective measures, communication-safety organization and monitoring and information security. e-mail: agchuk@yandex.ru.*

Andrei Sergeevich Korsunskii, *Candidate of Engineering; graduated from the Faculty of Radio-Communications at Ulyanovsk Branch of the Military Communications University; finished his post-graduate studies at the Marshal Budjonny Military Academy of Signal Corps; Chief Specialist at FRPC JSC 'RPA 'Mars'; an author of articles and inventions in the field of radio-electronics protection, communications, and information security as well as data transmission through wireless communication channels in information telecommunication systems. e-mail: aksspb@mail.ru.*

Vadim Gennadievich Fedorov, *graduated from Novocherkassk Military Academy of Communications; Adjunct of the Marshal Budjonny Military Academy of Signal Corps, an author of articles and inventions in the field of information security. e-mail: Vadim.fedorov.53@mail.ru.*

Abstract

The article deals with the problem of providing security and protection of information in information-telecommunication networks. It is well known that in order to ensure safety and information security, it is necessary to identify facts of hacks on computer networks with a high probability. There are a large number of systems and methods for detecting the destructive software attacks on a protected network. However, the existing technical solutions do not allow to achieve the required detection probability and recognition of types of destructive software attacks aimed at complex traffic shaping. The authors propose a way to protect the information-telecommunication networks against the effect of destructive complex traffic patterns through the introduction of a new distinction for detecting the class of computer network attacks and fixing it in time. The method provides an adaptive correction of the established access control rules taking into account the objective parameters of served traffic for the conservation of probability-time characteristics of subscriber service quality without increasing the performance of computing resources at the communication node.

Key words: objects being of critical importance, information-telecommunication networks security, protection against computer network attacks, destructive complex traffic.

Введение

В современном мире практически уже не осталось сфер деятельности, напрямую или опосредованно не связанных с использованием телекоммуникационных технологий. Степень их проникновения в системы государственного и военного управления, оборонную промышленность настолько велика, что можно с уверенностью утверждать: сегодня от инфотелекоммуникаций в полной мере зависит национальная безопасность страны. Очевидно, что в условиях чрезвычайно интенсивного развития инфотелекоммуникационных технологий существует множество так называемых критически важных объектов (КВО) с полным или частичным уровнем автоматизации систем управления. К сожалению, сложные инфотелекоммуникационные технологии сильно уязвимы для компьютерных атак. При этом атаки могут производиться удаленно, в том числе и из-за рубежа.

С точки зрения функционирования и эксплуатации автоматизированных систем управления (АСУ) КВО, необходимо отметить, что, хотя подобные системы и ограничены в подключении к ресурсам Единой сети электросвязи Российской Федерации (ЕСЭ РФ), полностью их изолировать практически невозможно. В противном случае придется пожертвовать функционалом АСУ либо ограничивать потребности должностных лиц, эксплуатирующих данные системы.

Исходя из этого, принципиальной особенностью применения инфотелекоммуникационной сети как технической основы АСУ КВО является использование ресурсов ЕСЭ РФ в качестве транспортной среды, предназначенной для обмена информацией и передачи трафика между взаимодействующими узлами сети [1, 2].

Однако в этой ситуации через открытую сеть открывается прямой доступ злоумышленникам к выделенной сети КВО и становится реальной возможность реализовать различные виды компьютерных атак.

Компьютерная атака – целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств.

Границы выделенной инфотелекоммуникационной сети определяются не установленным оборудованием, а реализованными способами защиты сети, т. е. необходимо ввести понятие логической контролируемой зоны. Под логической контролируемой зоной будем понимать виртуальную (логически выделенную) часть инфотелекоммуникационной среды, используемую для реализации защищаемых процессов, в пределах кото-

рой исключается несанкционированное изменение характеристик (параметров) защищаемого процесса.

Актуальные сетевые атаки

В настоящее время наиболее часто реализуемые сетевые компьютерные атаки имеют следующую классификацию:

- 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 [3].

Известно, что для обеспечения информационной безопасности необходимо с высокой вероятностью определять факты сетевых компьютерных атак. Имеется большое количество систем и способов обнаружения деструктивных программных воздействий на защищаемую сеть. Однако существующие технические решения не позволяют достичь необходимой вероятности обнаружения и распознавания типа деструктивных программных воздействий, имеющих своей целью формирование трафика сложной структуры.

Современная теория телетрафика, как правило, оперирует моделью пуассоновского потока (простейший поток). Информационный поток представляет собой точечные случайные процессы, статистические характеристики которых моделируют временную структуру поступления пакетов, порождаемых пользователями. Другими словами, имеется пакетная система связи, состоящая из источника и получателя пакетов данных, между которыми ведется передача информационного потока, структура которого соответствует пуассоновскому потоку с коэффициентом вариации интервалов времени между поступлениями отдельных пакетов $C_r \approx 1$ [4].

При этом под трафиком сложной структуры понимается трафик, у которого коэффициент вариации интервалов времени между поступлениями отдельных пакетов больше единицы $C_r > 1$. Такое формирование трафика сложной структуры может быть использовано для преднамеренного создания условий, направленных на повышение времени обработки информационных потоков в узлах маршрутизации, и как следствие, снижения своевременности обслуживания абонентов ниже значений, определяемых требованиями к системе связи.

Усложнение трафика по показателю коэффициента вариации с $C_r = 1$ до $C_r = 1{,}5$ увеличивает время обработки в узлах в 1,5–2 раза, а при достижении $C_r = 2$ время обработки увеличивается в 5–6 раз [5].

Реализация этого деструктивного программно-аппаратного воздействия обеспечивается за счет перехвата пакетов, формирования из перехваченных пакетов дополнительного трафика, который внедряется обратно в систему связи с целью формирования передаваемого по ней трафика сложной структуры.

Для того, чтобы сохранить вероятностно-временные характеристики качества обслуживания абонентов в условиях воздействия трафика сложной структуры, тривиальным решением является многократное увеличение вычислительных ресурсов на всех узлах маршрутизации. Это в свою очередь может привести к неэффективному использованию сети с неоправданными финансовыми затратами, так как деструктивное воздействие может возникать кратно либо вообще отсутствовать.

Таким образом, становится актуальной задача обеспечения адаптивной коррекции установленных правил разграничения доступа с учетом реальных характеристик обслуживаемого информационного потока с целью сохранения вероятностно-временных характеристик качества обслуживания абонентов в условиях воздействия трафика сложной структуры без увеличения производительности вычислительных ресурсов на узлах связи [6].

Разработка способа защиты от сетевых атак

Для решения поставленной задачи авторами статьи предлагается алгоритм адаптивной защиты инфотелекоммуникационных сетей от воздействия деструктивного трафика сложной структуры. Предложенный способ реализуется следующим образом.

В общем случае выделенная сеть представляет собой совокупность оконечного, периферийного и коммуникационного оборудований, которая имеет определенное количество каналов связи с другими выделенными сетями, используя при этом ресурсы ЕСЭ РФ.

Объединение выделенной сети 1 и ее пользователей $(1.1_1, 1.1_2, \ldots, 1.1_n)$ с адресами $(C_1, \ldots, C_n)$ с открытой сетью 4 носит характер использования ее в качестве транспортной магистрали для связи с другой выделенной сетью 2 и ее пользователями $(2.1_1, 2.1_2, \ldots, 2.1_n)$ с адресами $(S_1, \ldots, S_n)$ (рис. 1).

Открытая сеть 4 набором маршрутизаторов осуществляет транспортировку информационных потоков из выделенной сети 1 в выделенную сеть 2. При прохождении пакетов через открытую сеть 4 осуществляется их маршрутизация от источника к получателю в соответствии с IP-адресом назначения. В открытой сети 4 к одному из маршрутизаторов подключен комплекс деструктивного воздействия 4.1. Также через открытую сеть 4 открывается доступ к защищаемой сети 1 для пользователей $(3.1_1, 3.1_2, \ldots, 3.1_n)$ с адресами $(R_1, \ldots, R_n)$ других (нелегитимных) локальных сетей 3.

Для защиты внутренней сети 1, путем фильтрации нелегитимного трафика, в точке входа в сеть устанавливается шлюз-компьютер с межсетевым экраном 1.4, имеющий свой сетевой адрес (M), который настраивается таким образом, чтобы была обеспечена возможность контроля всего входящего и исходящего трафика.

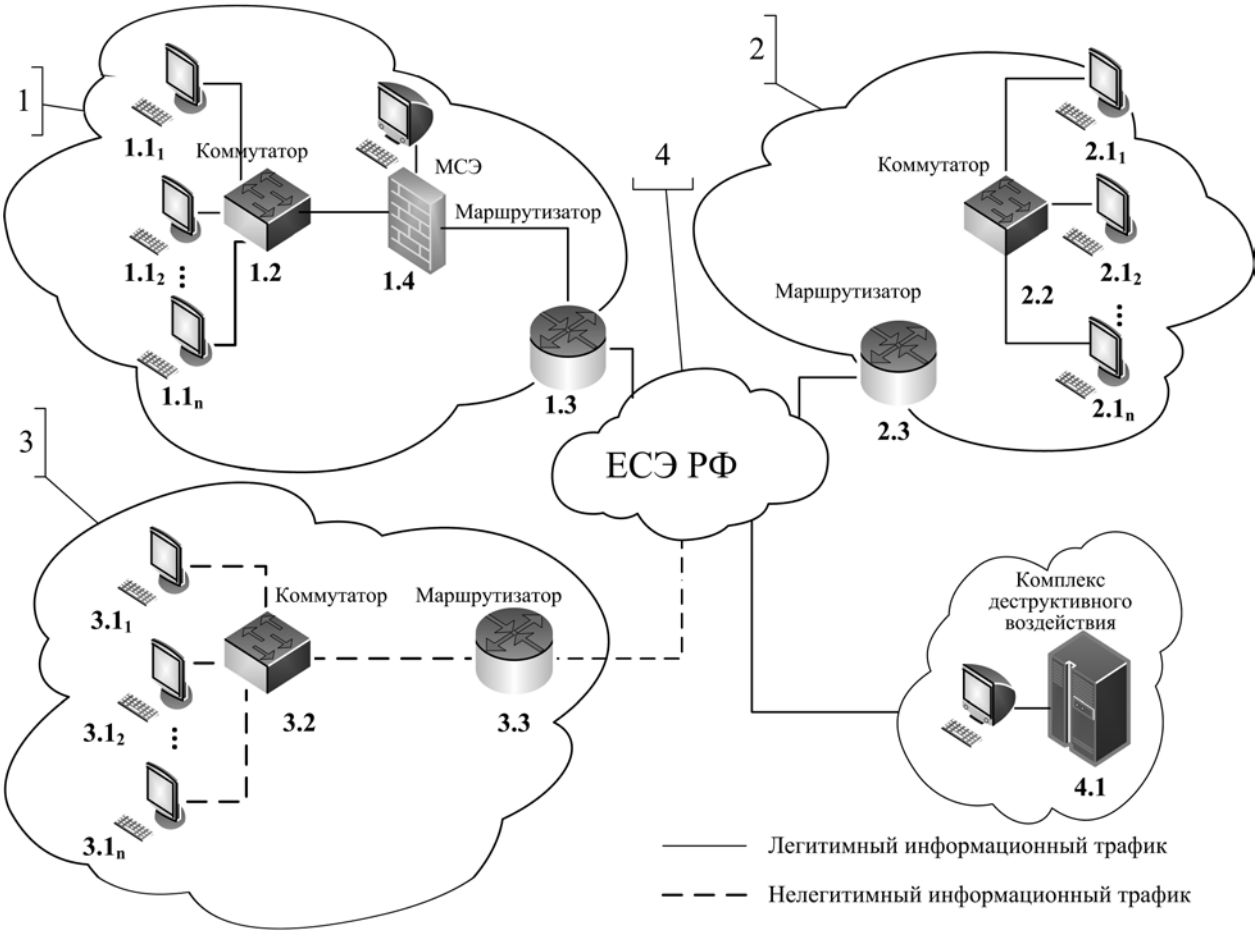

Рис. 1. Вариант схемы взаимодействия выделенных сетей через открытую сеть

В данной ситуации при конфигурации межсетевого экрана 1.4 выбирается стратегия защиты: «запрещено все, что не разрешено в явном виде». Такая стратегия облегчает администрирование межсетевого экрана (МСЭ) [7]. При этом возможно применение экранов, реализующих способы защиты персоны от психофизического воздействия. При данной организации сетевого взаимодействия представляется возможным использовать заявленный способ для адаптивной защиты от деструктивных программно-аппаратных воздействий путем их оперативного выявления на узлах маршрутизации.

Порядок взаимодействия в такой сети поясняется алгоритмом, представленным на рисунке 2. Предварительно формируется первоначальная база параметров легитимных абонентов (бл. 1), которая представляет собой некоторый список идентификаторов, в качестве которых в данном случае используют адреса отправителей и получателей, а также корректно установленные флаги SYN и ACK при запросах на установление связи. Затем задается пороговое значение коэффициента вариации интервалов времени между поступлениями отдельных пакетов для трафика от легитимного абонента $C_{\tau}^{пор} > 1$. Также задается время блокировки обнаруженного деструктивного сетевого трафика сложной структуры $t_{бл}$ (бл. 2). При получении пакета с установленным номером протокола $ICMP$ блокирует его на период установления легитимности (бл. 3).

Процесс функционирования протокола $ICMP$, обеспечивающего обратную связь в виде диагностических сообщений, посылаемых отправителю, подробно описан в [8]. Затем анализируется каждый поступающий из открытой сети пакет на предмет соответствия его параметров параметрам заранее сформированной базы легитимных пакетов (бл. 4). При установлении нелегитимности анализируемого пакета сетевые пакеты не доставляются получателю защищаемой сети, а весь трафик, поступающий от нелегитимного абонента, блокируется (бл. 5). В случае если параметры пакета полностью совпадают с базой параметров легитимных пакетов, измеряются характеристики легитимного трафика, а именно: временной интервал между соседними пакетами трафика τ и интенсивность поступления пакетов в информационном потоке λ (бл. 7).

Производится сбор данных этих характеристик трафика и их статистическая обработка для расчёта коэффициента вариации интервалов времени между поступлениями отдельных пакетов принятого трафика (бл .8) используя выражение:

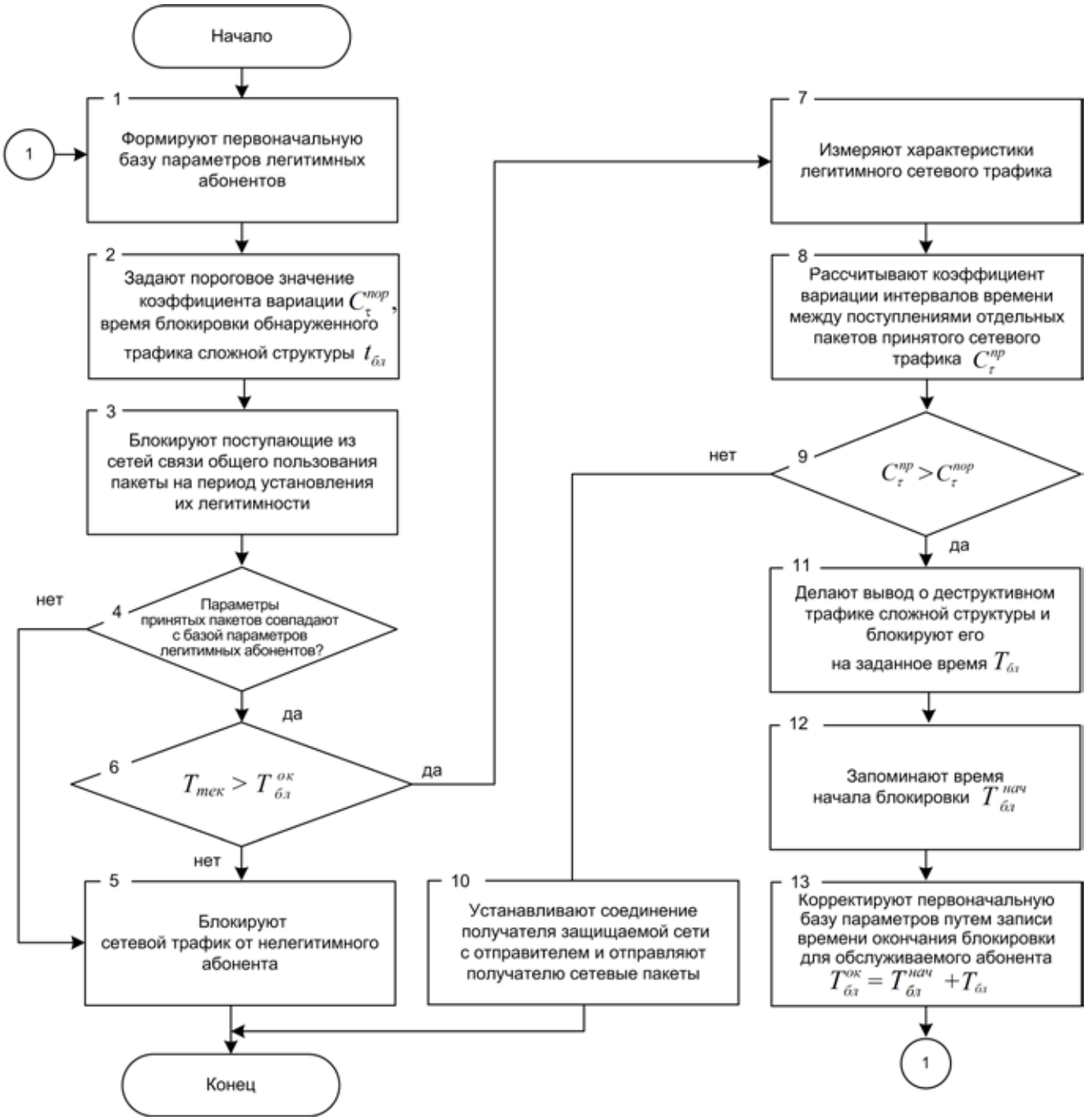

Рис. 2. Алгоритм реализации адаптивной защиты инфотелекоммуникационных сетей от воздействия деструктивного трафика сложной структуры

$$C_\tau^{пр} = \frac{\sigma_\tau}{m_\tau},$$

где σ_τ – среднее квадратическое отклонение распределения интервалов времени между поступлением пакетов трафика;

m_τ – математическое ожидание распределения интервалов времени между поступлением пакетов трафика.

Далее сравнивается значение коэффициента вариации $C_\tau^{пр}$ с заданным $C_\tau^{пор}$ для легитимного трафика (бл. 9). Если условие $C_\tau^{пр} > C_\tau^{пор}$ выполняется, то делается вывод о наличии деструктивного трафика сложной структуры и он блокируется на заданное время $T_{бл}$ (бл. 11), затем запоминается время начала блокировки $T_{бл}^{нач}$ (бл. 12), после чего корректируется первоначальная база параметров путем записи времени окончания блокировки $T_{бл}^{ок}$ для обслуживаемого абонента (бл. 13).

При этом время окончания блокировки определяется по формуле:

$$T_{бл}^{ок} = T_{бл}^{нач} + T_{бл},$$

где $T_{бл}^{нач}$ – метка времени в момент начала блокировки деструктивного трафика сложной структуры;

$T_{бл}$ – заданное время продолжительности блокировки обнаруженного деструктивного трафика сложной структуры.

Если с IP-адреса заблокированного абонента с обнаруженным деструктивным трафиком сложной структуры вновь поступили пакеты данных до времени окончания блокировки $T_{бл}^{ок}$ (бл. 6), то такой абонент считается нелегитимным и весь трафик от него вновь блокируется (бл. 5).

Если $C_{\tau}^{пр} \leq C_{\tau}^{пор}$, устанавливают соединение получателя защищаемой сети с отправителем (бл. 10) и сетевые пакеты доставляются получателю.

После истечения заданного времени блокировки $T_{бл}$, если с адреса ранее заблокированного абонента вновь поступили пакеты данных и анализ не выявил признаков деструктивного трафика сложной структуры, то такой абонент считается легитимным, устанавливается соединение получателя защищаемой сети с отправителем (бл. 10) и сетевые пакеты доставляются получателю.

Заключение

Таким образом, в предложенном способе за счет введения нового отличительного признака для определения деструктивного программного воздействия и фиксирования его во времени обеспечивается адаптивная коррекция установленных правил разграничения доступа с учетом реальных характеристик обслуживаемого трафика для сохранения вероятностно-временных характеристик качества обслуживания абонентов без увеличения производительности вычислительных ресурсов на узле связи.

СПИСОК ЛИТЕРАТУРЫ

1. Федоров В.Г., Стародубцев Ю.И Способ обнаружения источника сетевых атак на автоматизированные системы // Проблемы экономики и управления в торговле и промышленности. – 2016. – № 1. – С. 87–93.

2. Принципы безопасного использования инфраструктуры связи применительно к условиям техносферной войны / Ю.И. Стародубцев, А.Г. Чукариков, А.С. Корсунский, Е.В. Сухорукова // Интегрированные системы управления : сб. науч. тр. науч.-техн. конф. – Ульяновск, 2016. – С. 199–206.

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

4. Алиев Т.И. Основы моделирования дискретных систем – СПб. : СПбГУ ИТМО, 2009. – 363 с.

5. Макаренко С.И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика // Вопросы кибербезопасности. – 2014 – № 3. – С. 7–13.

6. Стародубцев Ю.И., Федоров В.Г. Способ адаптивной защиты выделенных сетей торгового объекта от воздействия деструктивного трафика сложной структуры // Проблемы экономики и управления в торговле и промышленности. – 2015. – № 3. – С. 57–63.

7. Липатников В.А., Стародубцев Ю.И. Защита информации – СПб. : ВУС, 2001. – 348 с.

8. Мельников Д.А. Информационные процессы в компьютерных сетях. Протоколы, стандарты, интерфейсы, модели. – М. : КУДИЦ-ОБРАЗ, 1999. – 256 с.

REFERENCES

1. Fedorov V.G., Starodubtsev Iu.I. Sposob obnaruzheniia istochnika setevykh atak na avtomatizirovannye sistemy [Method of Detecting Sources of Network Attacks on Automated Systems]. *Problemy ekonomiki i upravleniia v torgovle i promyshlennosti* [Problems of Economics and Management in Trade and Industry], 2016, no. 1, pp. 87–93.

2. Starodubtsev Iu.I., Chukarikov A.G., Korsunskii A.S., Sukhorukova E.V. Printsipy bezopasnogo ispolzovaniia infrastruktury sviazi primenitelno k usloviiam tekhnosfernoi voiny [Concepts of a Safe Use of Communication Infrastructure in the Context of Technosphere War]. *Integrirovannye sistemy upravleniia. Sb. nauch. tr. nauch.-tekhn. konf.* [Proc. of Sci. and Tech. Conf. on Integrated Control Systems]. Ulyanovsk, 2016, pp. 199–206.

3. Bazovaia model ugroz bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh. Rukovodiashchii document [Base Model of Personal Data Security Hazards While Processing in Personal Data Information Systems. Guidance Document]. Moscow, FSTEK Publ., 2008. 69 p.

4. Aliev T.I. *Osnovy modelirovaniia diskretnykh sistem* [Fundamentals of Sampling Simulation]. St. Petersburg, SPbGU ITMO Publ., 2009. 363 p.

5. Makarenko S.I. Prednamerennoe formirovanie informatsionnogo potoka slozhnoi struktury za schet vnedreniia v sistemu sviazi dopolnitelnogo imitatsionnogo trafika [Premeditated Formulation of the Traffic of Difficult Structure Due to Implementation in the Communication System of Additional Imitative Traffic]. *Voprosy kiberbezopasnosti* [Security Issues], 2014, no. 3, pp. 7–13.

6. Starodubtsev Iu.I., Fedorov V.G. Sposob adaptivnoi zashchity vydelennykh setei torgovogo obiekta ot vozdeistviia destruktivnogo trafika slozhnoi struktury [Method of Adaptive Protection of Dedicated Networks of Commercial Facility Against the Effects of Destructive Complex Traffic Patterns]. *Problemy ekonomiki i upravleniia v torgovle i promyshlennosti* [Problems of Economics and Management in Trade and Industry], 2015, no. 3, pp. 57–63.

7. Lipatnikov V.A., Starodubtsev Iu.I. *Zashchita informatsii* [Information Security]. St. Petersburg, VUS Publ., 2001. 348 p.

8. Melnikov D.A. *Informatsionnye protsessy v kompiuternykh setiakh. Protokoly, standarty, interfeisy, modeli* [Information Processes in Computer Networks. Protocols, Standards, Interfaces, Models]. Moscow, KUDITs-OBRAZ Publ., 1999. 256 p.