**Федоров Вадим Геннадиевич,**
к.т.н., слушатель Военной академии связи,
Санкт-Петербург

**Федорова Светлана Викторовна,**
К.т.н. преподаватель Военной академии связи,
Санкт-Петербург

**Ефимов Андрей Валерьевич,**
слушатель Военной академии связи,
Санкт-Петербург

# СПОСОБ АДАПТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ ОТ ДЕСТРУКТИВНЫХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ

**Аннотация:** В статье рассмотрена проблема обеспечения безопасности и защиты информации в информационно-телекоммуникационных сетях. Предложен способ их защиты от воздействия деструктивного трафика сложной структуры посредством введения нового отличительного признака для определения этого класса сетевых компьютерных атак и фиксированием его во времени.

**Ключевые слова:** защищенность информационно-телекоммуникационных сетей, события безопасности, защита от компьютерных атак.

Мировые тенденции развития в области информатизации и связи показывают, что на базе цифровых методов передачи, обработки, хранения, представления и защиты информации быстрыми темпами идет процесс взаимопроникновения и «сращивания» информационных и телекоммуникационных систем не только на уровне технологий их разработки и эксплуатации, но и их структурного и функционального объединения. Роль защиты информации на всех этапах функционирования информационно-телекоммуникационных систем остается приоритетной.

Несанкционированные воздействия на компьютерные сети как коммерческих организаций и федеральных структур, так и критически важных объектов осуществляется на основе данных, добываемых организованным нарушителем с использованием средств компьютерной разведки. С точки зрения функционирования и эксплуатации информационно-телекоммуникационных сетей специального назначения (ИТКС СН) необходимо отметить тот факт, что, хотя подобные системы и ограничены в подключении к сетям общего пользования, полностью их изолировать практически невозможно. В противном случае придется пожертвовать функционалом автоматизированных систем, либо ограничивать потребности должностных лиц, эксплуатирующих данные системы. [1-3].

В общем случае информационно-телекоммуникационная сеть представляет собой совокупность оконечного, периферийного и коммуникационного оборудования. Каждая информационно-телекоммуникационная сеть имеет определенное количество каналов связи с другими выделенными сетями. Принципиальной особенностью их применения является использование ресурсов открытой сети как транспортной среды, предназначенной для обмена информацией и передачи трафика между взаимодействующими узлами информационно-телекоммуникационной сети торгового объекта [1-3]. Трафик – нагрузка, создаваемая потоком вызовов, сообщений, пакетов и сигналов, поступающих на средства связи [4].

Современная теория телетрафика, как правило, оперирует моделью пуассоновского потока (простейший поток) [5]. 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 Cτ≈1 [6].

Вместе с тем, в этой ситуации через открытую сеть открывается прямой доступ злоумышленникам к выделенной сети объекта и делает реальным 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 [7].

Границы выделенной информационно-телекоммуникационной 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 которой исключается несанкционированное изменение характеристик (параметров) защищаемого процесса. В настоящее время наиболее часто реализуемые компьютерные атаки классифицируются на [8]:

- 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.

Цель деструктивных программных воздействий – организация канала утечки информации, блокирование, модификация, уничтожение информационных ресурсов, блокирование средств защиты информации торгового объекта.

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. При этом под трафиком сложной структуры понимается трафик, у которого коэффициент вариации интервалов времени между поступлениями отдельных пакетов больше единицы $C_\tau$>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.

Увеличение сложности трафика по показателю коэффициента вариации с $C_\tau$=1 до 1,5 увеличивает время обработки в узлах 1,5-2 раза, а при увеличении до $C_\tau$=2 время обработки увеличивается в 5-6 раз. [9].

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.

Для решения этой задачи авторами статьи предлагается способ адаптивной защиты информационно-телекоммуникационных сетей от деструктивных программных воздействий.

Предложенный способ реализуется следующим образом.

В общем случае выделенная сеть представляет собой совокупность оконечного, периферийного и коммуникационного оборудования, которая имеет определенное количество каналов связи с другими выделенными сетями. Вариант схемы приведен на рисунке 1.

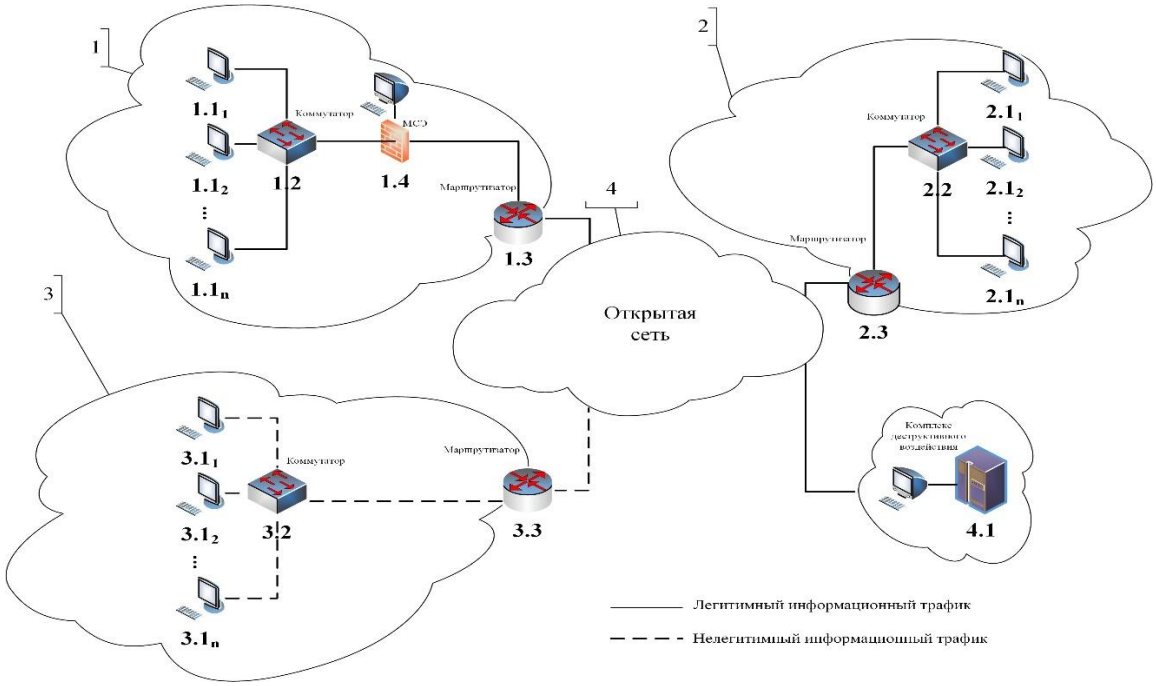


Рис. 1 – Вариант схемы взаимодействия выделенных сетей через открытую сеть

Объединение выделенной сети 1 и ее пользователей (1.11, 1.12,…, 1.1n) с адресами (C1, …, Cn) с открытой сетью 4 носит характер использования ее в качестве транспортной магистрали для связи с другой выделенной сетью 2 и ее пользователями (2.11, 2.12,…, 2.1n) с адресами (S1,…, Sn) (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 его 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 (3.11, 3.12,…, 3.1n) с адресами (R1,…, Rn) других (нелегитимных) локальных сетей 3.

Для защиты внутренней сети 1, путем фильтрации нелегитимного трафика, в точке входа в сеть устанавливают 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.

В данной ситуации, при конфигурации межсетевого экрана 1.4 выбирают стратегию защиты: «запрещено все, что не разрешено в явном виде». Такая стратегия облегчает администрирование межсетевого экрана [10]. 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 далее. Предварительно формируют первоначальную базу параметров легитимных абонентов, 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. Задают пороговое значение коэффициента вариации интервалов времени между поступлениями отдельных пакетов для трафика от легитимного абонента $C_{\tau\,пор}>1$. Задают время блокировки обнаруженного деструктивного сетевого трафика сложной структуры $t_{бл}$ . При получении пакета с установленным номером протокола ICMP (Internet Control Message Protocol, протокол управляющих сообщений Интернет) блокируют его на период установления легитимности.

Процесс функционирования протокола ICMP, обеспечивающего обратную связь в виде диагностических сообщений, посылаемых отправителю подробно описан [11]. Затем анализируют каждый поступающий из открытой сети пакет на предмет соответствия его параметров параметрам заранее сформированной базы легитимных пакетов. При установлении нелегитимности анализируемого пакета сетевые пакеты не доставляют получателю защищаемой сети, а весь трафик, поступающий от нелегитимного абонента блокируют. В случае если параметры пакета полностью совпадают с базой параметров легитимных пакетов измеряют характеристики легитимного трафика, а именно временной интервал между соседними пакетами трафика $\tau$ и интенсивность поступления пакетов в информационном потоке $\lambda$ . Производят сбор данных этих характеристик трафика и их статистическую обработку для расчёта коэффициента вариации интервалов времени между поступлениями отдельных пакетов принятого трафика $C_{\tau\,пр}$. по формуле [6]:

$$C_{\tau} = \frac{\sigma_{\tau}}{m_{\tau}} \quad (1)$$

Где $\sigma_{\tau}$ – среднее квадратическое отклонение распределения интервалов времени между поступлением пакетов трафика, $m_{\tau}$ – математическое ожидание распределения интервалов времени между поступлением пакетов трафика.

Сравнивают значение коэффициента вариации $C_{\tau\,пр}$ с заданным $C_{\tau\,пор}$ для легитимного трафика. Если условие $C_{\tau\,пр} > C_{\tau\,пор}$ выполняется, то делают вывод о наличии деструктивного трафика сложной структуры и блокируют его на заданное время $t_{бл}$ , запоминают время начала блокировки $t_{н.бл}$ , после чего корректируют первоначальную базу параметров путем записи времени окончания блокировки $t_{ок.бл}$ для обслуживаемого абонента.

При этом время окончания блокировки определяется по формуле:

$$t_{ок.бл} = t_{н.бл} + t_{бл} \quad (2)$$

Где $t_{н.бл}$ – 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 $t_{ок.бл}$ , то такой абонент считается нелегитимным и весь трафик от него вновь блокируется.

Если $C_{\tau\ пр} \leq C_{\tau\ пор}$ устанавливают соединение получателя защищаемой сети с отправителем и сетевые пакеты доставляются получателю.

После истечения заданного времени блокировки $t_{бл}$, если с адреса раннее 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 и сетевые пакеты доставляются получателю.

Таким образом, в предложенном способе за счет введения нового отличительного признака для определения деструктивного программного воздействия и фиксированием 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. Стародубцев Ю.И., Чукариков А.Г., Корсунский А.С., Федоров В.Г. Способ защиты инфотелекоммуникационных сетей критически важных объектов от сетевых компьютерных атак / Автоматизация процессов управления. 2018. № 1 (51). с. 14-19.

2. Федоров В.Г., Федорова С.В., Спицын О.Л. Способ выделения структурно-топологических неоднородностей заданного фрагмента сети связи / I-methods. 2019. Т. 11. № 2 с. 1-13.

3. Стародубцев Ю.И., Сухорукова Е.В., Яблоков Д.Ю. Способ повышения защищенности элементов территориально-распределенных информационно-телекоммуникационных систем / Проблемы экономики и управления в торговле и промышленности, 2015. - №119. – с. 95-101.

4. Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи» (ред. от 01.03.2015 г.) //«Российская газета», 10.07.2003, №135

5. Крылов В.В., Самохвалова С.С. Теория телетрафика и ее приложения. – СПб.: БВХ-Петербург, 2005. – 288 с.

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

7. ГОСТ Р 50.1.056-2005 Техническая защита информации. Основные термины и определения.

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

9. Макаренко С.И. Преднамеренное формирование информационного потока сложной структуры за счет внедрения в систему связи дополнительного имитационного трафика. Научно-практический журнал «Вопросы кибербезопасности» №3 2014. – 76 с.

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

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