УДК 004.738.5.057.4

Метод обнаружения сетевого перехвата информационного трафика информационно-телекоммуникационной сети

В.В. Бухарин, А.В. Кирьянов, Ю.И. Стародубцев, С.С Трусков

Аннотация:

В статье рассмотрен метод обнаружения сетевого анализа информационного трафика ИТКС. Разработанный метод позволяет повысить достоверность обнаружения компьютерных атак, в том числе и пассивных атак

на ИТКС путем передачи проверочных пакетов и анализа ответных пакетов от маршрутизаторов внешней сети, используемых на маршруте передачи пакетов сообщения.

Ключевые слова:

анализ сетевого трафика; информационно-телекоммуникационная сеть; IP протокол.

В настоящее время информационно-телекоммуникационные сети (ИТКС) имеют множество уязвимостей, возникших как при разработке системного программного обеспечения, так и при неправильной конфигурации оборудования. Наличие угроз безопасности в ИТКС делает реальным возможность злоумышленникам реализовать различные виды атак. Границы ИТКС 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 ИТКС должна иметь иерархическую и системно-взаимоувязанную систему защиты. Вышеперечисленные компьютерные атаки могут влиять на достоверность получаемой информации в связи, с чем актуальной является задача обнаружения подмены доверенного объекта ИТКС.

Известен метод защиты от компьютерных атак, включающий следующую последовательность действий [2]. Наблюдение за информационным потоком адресованных абоненту ИТКС пакетов сообщений, включающее постоянно возобновляемый подсчет числа пакетов, выполняемый в пределах серии пакетов, поступающих из канала связи (КС) подряд друг за другом через промежутки времени не более заданного. При этом проверку поступающих пакетов данных на соответствие заданным правилам выполняют каждый раз, когда размер очередной наблюдаемой серии достигает критического числа пакетов.

Недостатками данного способа являются, узкая область применения, что обусловлено его предназначением в основном для защиты от подмены одного из участников соединения, и недостаточная достоверность при обнаружении других типов компьютерных атак.

Известен метод, позволяющий по изменению состояния элемента ИТКС обнаруживать компьютерные атаки [3]. В частности, преобразуют результаты допусковой оценки разнородных динамических параметров в соответствующие информационные сигналы с обобщением по всему множеству параметров в заданном временном интервале и определяют относительную величину и характер изменения интегрального состояния многопараметрического элемента ИТКС.

Недостатком данного способа является узкая область применения, обусловленная тем что, несмотря на возможность оперативной диагностики технического и функционального состояний многопараметрического элемента ИТКС, в нем применяют ограниченную совокупность признакового пространства, что создает условия для пропуска удаленных компьютерных атак [4] и, как следствие, приводит к снижению устойчивости функционирования ИТКС.

Известен метод защиты от компьютерных атак [5], заключается в том, что принимают из КС i-ый пакет, где i=1, 2, 3,..., и запоминают его. Принимают (i+1)-ый пакет, запоминают его. Выделяют из заголовка i-го и (i+1)-го пакетов идентификационные признаки, анализируют их на предмет совпадения, по результатам анализа принимают решение о факте наличия компьютерной атаки.

Недостатком данного метода является относительно низкая устойчивость

функционирования ИТКС в условиях воздействия компьютерных атак, связанная с тем, что сравнением двух пакетов сообщений – последующего и предыдущего, распознается только одно семейство компьютерных атак – "шторм" ложных запросов на установление соединения, тогда как компьютерные атаки других типов, обладающие высокими деструктивными возможностями, не распознаются.

Наиболее близким по технической сущности к предлагаемому методу является способ защиты информационно-вычислительных сетей от компьютерных атак [6]. Способ заключается в следующих действиях: принимают *i*-й, где *i*=1, 2, 3..., пакет сообщения из канала связи, запоминают его, принимают (*i*+1)-й пакет сообщения, запоминают его, выделяют и запомненных фрагментированных пакетов сообщений характеризующие их параметры, вычисляют необходимые параметры для сравнения принятых фрагментированных пакетов и по результатам сравнения принимают решение о факте наличия или отсутствия компьютерной атаки.

Недостатком данного способа является относительно низкая достоверность обнаружения компьютерных атак, обусловленная тем, что определяются только активные компьютерные атаки, что может привести к перехвату передаваемых данных в ИТКС по внешней сети.

Целью предлагаемого метода является обнаружение сетевого анализа информационного трафика ИТКС, обеспечивающего, повышение достоверности обнаружения компьютерных атак на ИТКС, за счет определения информации о ведении всех видов компьютерных атак, в том числе и пассивных, путем передачи проверочных пакетов и анализа ответных пакетов от маршрутизаторов внешней сети, используемых на маршруте передачи пакетов сообщения.

Существующие угрозы безопасности информации могут быть реализованы путем использования протоколов межсетевого взаимодействия при построении распределенной ИТКС состоящей из нескольких сегментов, которые взаимодействуют через внешнюю сеть (сеть связи общего пользования). При этом данные угрозы реализуются за счет проведения компьютерных атак, которые могут быть активными и пассивными. Особую опасность представляют пассивные компьютерные атаки, которые не оказывается непосредственное влияние на работу ИТКС, но при этом могут быть нарушены установленные правила разграничения доступа к данным или сетевым ресурсам. Примером является компьютерная атака «Анализ сетевого трафика», направленная на прослушивание каналов связи и перехват передаваемой информации [1].

В предлагаемом изобретении используется принцип трассировки маршрута

прохождения пакетов по внешней сети, заложенный в процедурной характеристике протокола IP и ICMP.

Реализацию заявленного метода можно пояснить на схеме ИТКС, показанной на рисунке 1.

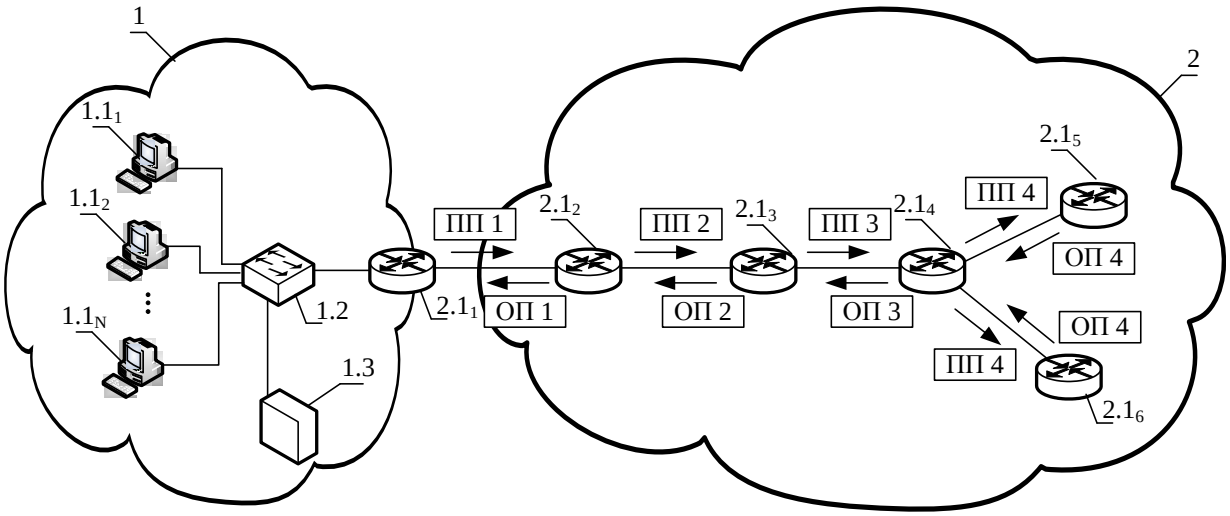

Рисунок 1 - Схема, поясняющая порядок передачи тестовых пакетов и приема ответных пакетов в ИТКС

Защищаемая ИТКС 1 подключена к внешней сети 2 посредством маршрутизатора 2.1_1. В общем случае защищаемая ИТКС 1 представляет собой совокупность ПЭВМ 1.1_1–1.1_N, периферийного и коммуникационного оборудования 1.2 и 1.3, объединенного физическими линиями связи. Все эти элементы имеют идентификаторы, в качестве которых в наиболее распространенном стеке протоколов TCP/IP используются сетевые адреса (IP-адреса). Внешняя сеть представлена набором маршрутизаторов 2.1_2–2.1_6, осуществляющих транспортировку информационных потоков из одного сегмента защищаемой ИТКС в другой.

Структура пакетов сообщений известна, как известен и принцип передачи пакетов в ИТКС. Например, на рисунке 2 представлена структура заголовка IP-пакетов сообщений, где выделены поля: времени жизни пакета, адресов отправителя и получателя пакета сообщений [7].

При прохождении пакетов через внешнюю сеть осуществляется его маршрутизация от источника к получателю в соответствии с IP адресом назначения. Кроме того, источник

задает время жизни пакета, и при прохождении каждого маршрутизатора данное время уменьшается на единицу. Данное поле позволяет уменьшить возможность перегрузки сети.

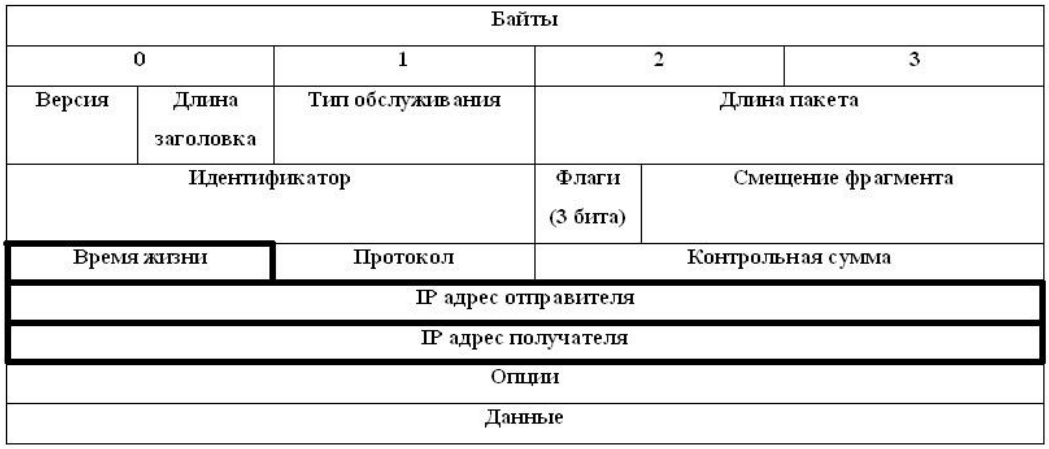

Рисунок 2 - Заголовок IP дейтограммы

Максимальное значение времени жизни является 255, так как под это поле в заголовке IP пакета отводится два байта. Соответственно, если маршрутизатор обнаруживает пакет с нулевым значение поля времени жизни, он его удаляет и сообщает об этом источнику данного пакета специально сформированным пакетом протокола ICMP (рисунок 3) [8].

Рисунок 3 – Заголовок IP и ICMP дейтаграммы

Таким образом, на один удаленный пакет источник пакета получит одно ICMP сообщение от промежуточного маршрутизатора о данном действии, если принято два и более ICMP сообщений от разных промежуточных маршрутизаторов это означает

тиражирование пакетов, что в свою очередь является признаком возможного перехвата передаваемого трафика.

На рисунке 1 поясняется порядок передачи проверочных пакетов (ПП) и приема ответных пакетов (ОП) по маршруту включающем четыре маршрутизатора 2.1_2–2.1_5. Первый проверочный пакет ПП 1 со значением поля времени жизни пакета равным одному переприему, передается по внешней сети 2 до маршрутизатора 2.1_2, на котором происходит удаление данного пакета и передача ответного пакета ОП 1 источнику, имеющего формат протокола ICMP и содержащего информацию об удаленном пакете.

В случае приема только одного ответного пакета ОП 1 формируется следующий проверочный пакет ПП 2 со значением поля времени жизни пакета равным двум, т.е. пакет будет удален на втором транзитном маршрутизаторе, и передается по внешней сети 2. На маршрутизаторе 2.1_3 данный пакет удаляется и передается ответный пакет ОП 2 на ИТКС 1.

При приеме только одного ответного пакета ОП 2 формируют следующий проверочный пакет ПП 3 со значением поля времени жизни пакета равным трем переприемам и передается по внешней сети 2. На маршрутизаторе 2.1_4 данный пакет удаляется и передается ответный пакет ОП 3 на ИТКС 1.

В случае приема только одного ответного пакета ОП 3 формируется следующий проверочный пакет ПП 4 со значением поля времени жизни пакета равным четырем переприемам и передается по внешней сети 2. На маршрутизаторе 2.1_5 данный пакет удаляется и передается ответный пакет ОП 4 на ИТКС 1. Кроме того, при перехвате передаваемого трафика с маршрутизатора 2.1_6, не принадлежащего маршруту передачи проверочных пакетов, будет так же передан ответный пакет ОП 4 содержащий информацию об удаленном пакете ПП 4 на ИТКС 1.

При получении двух ответных пакетов ОП 4, выполняется условие $K > K_{\text{доп}}$, при котором принимается решение о наличии компьютерной атаки, и прекращается дальнейшая передача проверочных пакетов.

На рисунке 4 представлена блок-схема последовательности действий, реализующих метод обнаружения сетевого анализа информационного трафика ИТКС.

После того как будут сформированы массивы $\{P\}$, $\{D\}$, $\{I\}$, а также список доверенных адресов отправителей и получателей сообщений (блок 1–3 рис.4), задают значение допустимого количества ICMP сообщений на пакет удаленный во внешней сети $K_{\text{доп}} = 1$ (блок 4 рис.4). Затем формируют проверочный пакет со значением поля временем жизни равным единице, заданными адресами источника и получателя сообщения, запоминают его в массив P_{ij} и передают его в канал связи через внешнюю сеть 2

(блок 5–11 рис.4).

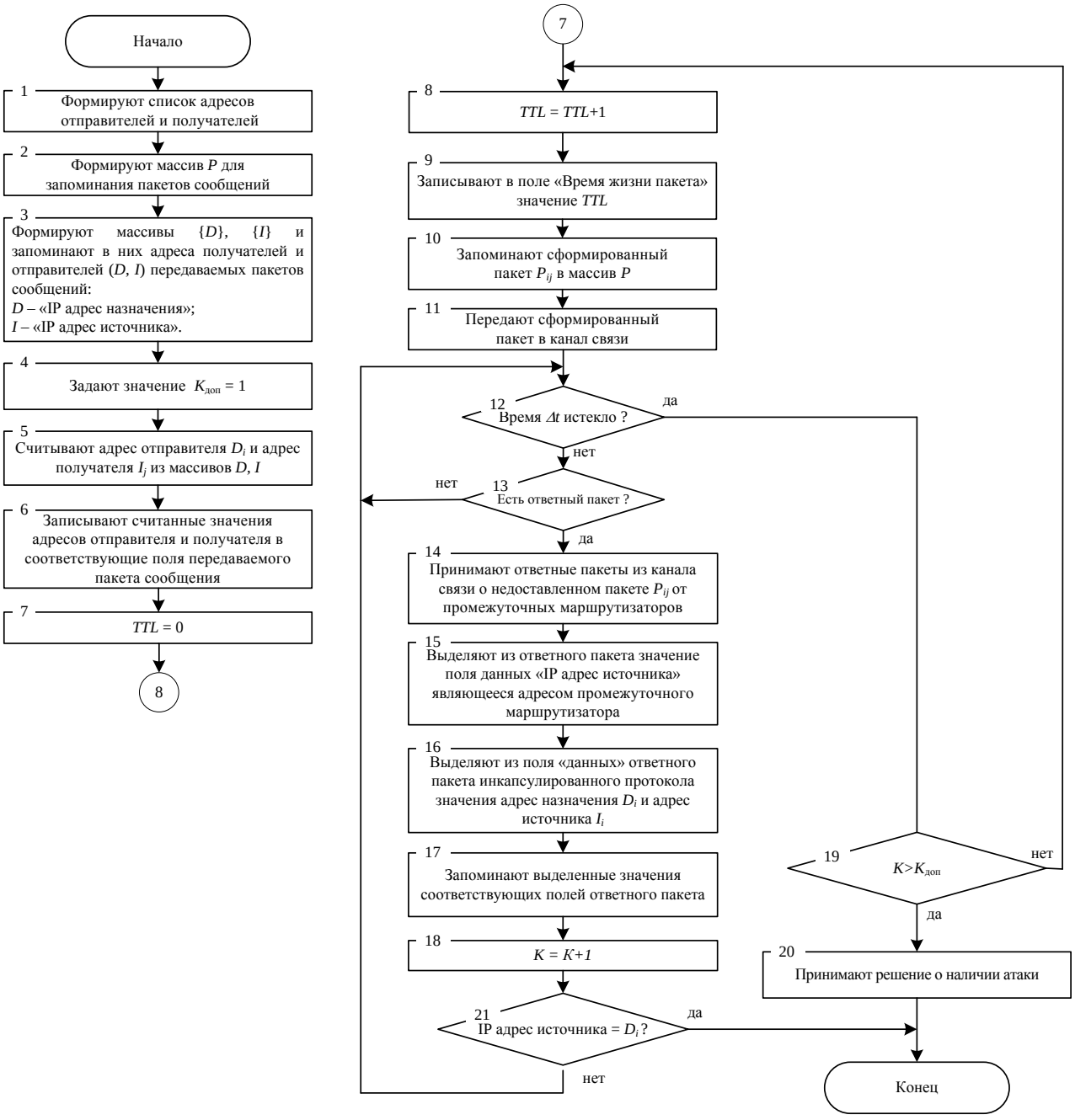

Рисунок 4 - Блок-схема последовательности действий метода обнаружения сетевого анализа информационного трафика ИТКС

Осуществляется прием ответных пакетов протокола ICMP из канала связи о недоставленном пакете P_{ij} от промежуточного маршрутизатора за время Δt (блок 12–17 рис.4). Если, при подсчете количества ответных пакетов, их получено больше чем $K_{доп}$ принимается решение о наличии компьютерной атаки (блок 18–20 рис.4).

Иначе производится увеличение значения поля времени жизни пакета на единицу и отправка очередного проверочного пакета (блок 8–11 рис.4). Проверка наличия компьютерной атаки осуществляется до выполнения условия, при котором проверочный пакет достиг конечного узла назначения (блок 21 рис.4).

Возможность реализации сформулированного технического результата была проверена путем машинного моделирования. При передаче проверочных пакетов размером 120 байт через внешнюю сеть, содержащую 10 транзитных маршрутизаторов, было передано 10 ПП и соответственно получено 10 ОП. На передачу ПП и получение ОП затрачивается в среднем от 70 до 120 миллисекунд. Таким образом, при осуществлении одной проверки, передается 1200 байт за секунду. При использовании канала передачи данных с пропускной способностью в 2 Мбит/с, нагрузка созданная проверочным потоком, составляет 0,005 процента от максимальной пропускной способности, что подтверждает возможность применения метода в существующих ИТКС.

Таким образом, разработанный метод обнаружения сетевого анализа информационного трафика ИТКС, за счет определения пассивных атак, путем передачи проверочных пакетов и анализа ответных пакетов от маршрутизаторов внешней сети, используемых на маршруте передачи пакетов сообщения, позволяет повысить достоверность обнаружения компьютерных атак на ИТКС.

Библиографический список:

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

2. Способ обнаружения удаленных атак в компьютерной сети: пат. 2179738 Рос. Федерация. № 2000111077/09; заявл. 24.04.00; опубл. 20.02.02, Бюл. № 3. 12 с.

3. Способ оперативного динамического анализа состояний многопараметрического объекта: пат. 2134897 Рос. Федерация. № 98106597/09; заявл. 31.03.98; опубл. 20.08.99, Бюл. № 9. 14 с.

4. Медведовский И.Д. и др. Атака на Internet. – М.: ДМК, 1999. – 336 с.: ил.

5. Устройство поиска информации: пат. 2219577, Рос. Федерация. № 2002111059/09; заявл. 24.04.02; опубл. 20.12.03, Бюл. № 21. 15 с.

6. Способ защиты информационно-вычислительных сетей от компьютерных атак: пат. 2285287, Рос. Федерация. № 2005109585/09; заявл. 04.04.05; опубл. 10.10.06, Бюл. № 28. 19 с.

7. Интернет протокол. URL:http://www.ietf.org/rfc/rfc791.txt (дата обращения: 12.05.2012).

8. Протокол межсетевых управляющих сообщений. URL:http://www.ietf.org/rfc/rfc792.txt (дата обращения: 12.05.2012).

Сведения об авторах:

Бухарин Владимир Владимирович, докторант Военной академии связи им. Буденного, к.т.н.
Санкт-Петербург, Тихорецкий пр. д.3, 194064;
тел.:(812)556-93-41, 8-9643836628, e-mail:bobah_buch@mail.ru.

Кирьянов Александр Владимирович, адъюнкт Военной академии связи им. Буденного, к.т.н.
Санкт-Петербург. Тихорецкий пр. д.3, 194064;
тел.: (812)556-93-41, e-mail:alex1175@rambler.ru.

Стародубцев Юрий Иванович, профессор Военной академии связи им. Буденного, д.в.н., заслуженный деятель науки РФ, профессор.
Санкт-Петербург, Тихорецкий пр. д.3, 194064;

Трусков Станислав Сергеевич, начальник отдела Федеральной службы охраны России, к.в.н.
Санкт-Петербург, e-mail:777.ru73@mail.ru.