УДК 004.738.5.057.4

Способ защиты информационно-вычислительных сетей от компьютерных атак

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

Аннотация:

Рассмотрен способ защиты информационно-вычислительной сети при возникновении нарушений внешнего периметра системы защиты информации, реализуемых посредством осуществления компьютерных атак. Данный способ позволяет повысить оперативность обнаружения компьютерной атаки за счет использования трассировки маршрутов передачи пакетов.

Ключевые слова:

защита информационно-вычислительной сети, компьютерная атака, трассировка маршрута, IP протокол.

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-телекоммуникационной системы остается приоритетной.

На этапе организации несанкционированного доступа к защищаемой сети, одной из задач является нарушение внешнего периметра системы защиты информации (СЗИ), реализуемое посредством применения компьютерных атак. Сетевая компьютерная атака – заранее спланированное целенаправленное воздействие на определенные объекты компьютерных сетей программными и аппаратными средствами через установление

соединения на сетевом уровне или попытки установления соединения на канальном или сетевом уровне ЭМВОС с объектом данного воздействия. Цель атаки – организация канала утечки информации, блокирование, модификация, уничтожение информационных ресурсов, блокирование СЗИ объекта.

Существуют и активно развиваются СЗИ которые реализуют различные способы защиты от компьютерных атак. Так, один из них, включает следующую последовательность действий: 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 [1].

Недостатком данного способа является низкая оперативность обнаружения компьютерной атаки, обусловленная выполнением соответствующих действий по обнаружению уже в процессе осуществления компьютерной атаки, что может привести к несанкционированному воздействию на информационно-вычислительную сеть.

Целью предлагаемого технического решения является разработка способа защиты информационно-вычислительных сетей, от компьютерных атак, обеспечивающего, повышение оперативности обнаружения компьютерной атаки на информационно-вычислительную сеть.

Реализация заявленного способа поясняется блок-схемой на рисунке 1.

Непосредственная реализация способа объясняется следующим образом:

1. Формируют массив *P* для запоминания поступающих из канала связи IP-пакетов сообщений.

2. Формируют массивы *D, I, T* и *O*, для запоминания параметров выделенных из запомненных пакетов сообщений соответственно:

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»;

O – для запоминания значений поля данных «Опции».

В предлагаемом решении используют функции протокола IP, применяемые при передаче пакетов по сети. Заголовок пакета протокола IP, представленный на рисунке 2, содержит определенное количество полей. В полях «IP адрес назначения» и «IP адрес

источника» будут находиться 32-битные последовательности, определяющие логические адреса назначения и источника пакета сообщения необходимые для передачи его по ИВС.

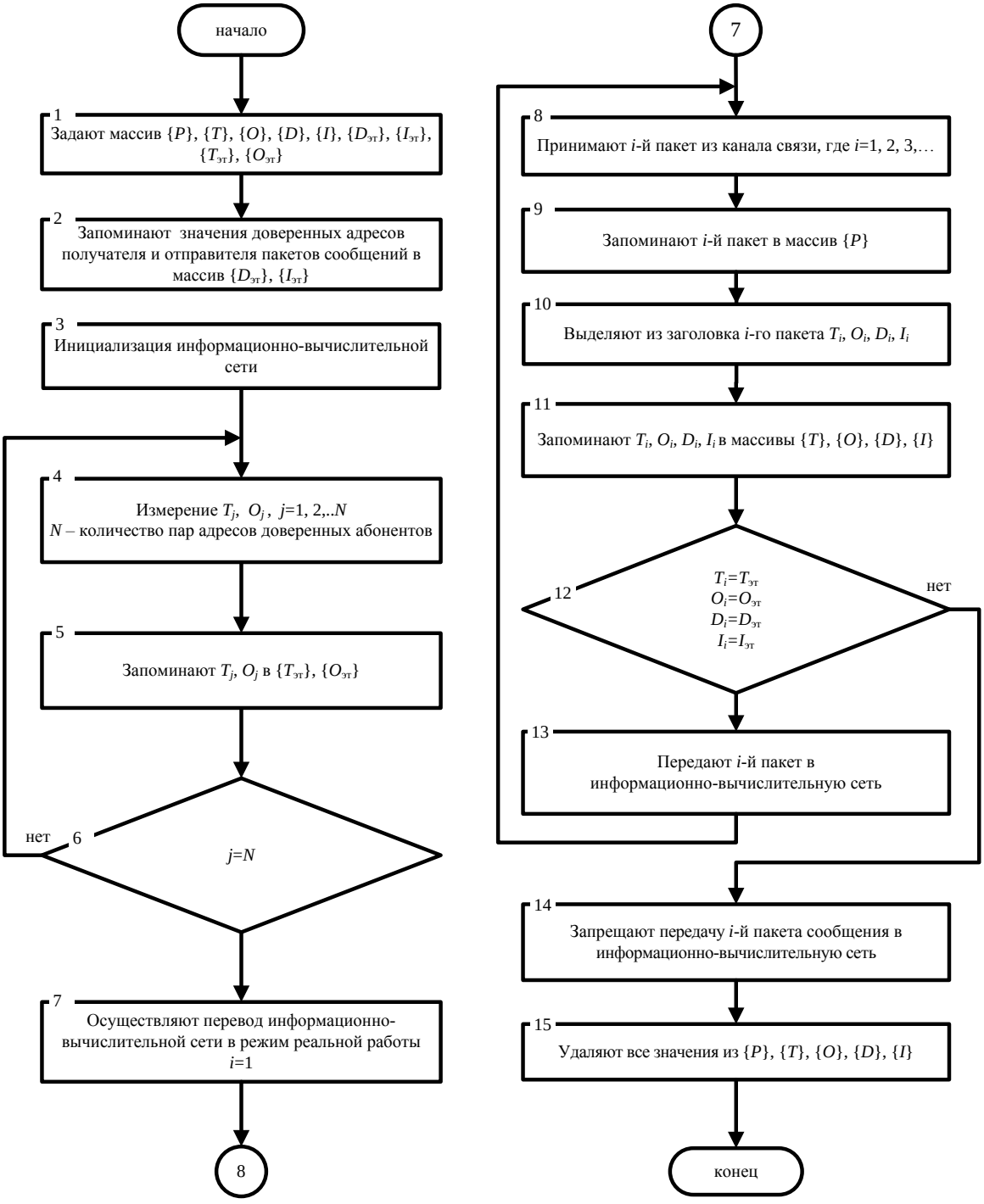

Рисунок 1 - Блок-схема способа защиты ИВС от компьютерных атак

Поле «Время жизни пакета» определяет максимальное время существования дейтаграммы в сети.

Поле «Опции» является необязательным и имеет переменную длину. Поддержка опций должна реализоваться во всех модулях IP (узлах и маршрутизаторах). Стандартом определены 8 опций. В предлагаемом решении используется опция – «запись маршрута» [2].

<table>
<tr><td colspan="5">Байты</td></tr>
<tr><td colspan="2">0</td><td>1</td><td colspan="2">2</td><td>3</td></tr>
<tr><td>Версия</td><td>Длина заголовка</td><td>Тип обслуживания</td><td colspan="3">Длина пакета</td></tr>
<tr><td colspan="3">Идентификатор</td><td>Флаги (3 бита)</td><td colspan="2">Смещение фрагмента</td></tr>
<tr><td colspan="2">Время жизни</td><td>Протокол</td><td colspan="3">Контрольная сумма</td></tr>
<tr><td colspan="6">IP адрес отправителя</td></tr>
<tr><td colspan="6">IP адрес получателя</td></tr>
<tr><td colspan="6">Опции</td></tr>
<tr><td colspan="6">Данные</td></tr>
</table>

Рисунок 2 - Логическая характеристика протокола IP v4

3. Формируют массивы $D_{эт}$, $I_{эт}$ для запоминания эталонных параметров выделенных из запомненных пакетов сообщений:

$D_{эт}$ – значений поля данных «IP адрес назначения»;

$I_{эт}$ – значений поля данных «IP адрес источника».

4. Формируют массивы $T_{эт}$, $O_{эт}$ для запоминания эталонных параметров выделенных из запомненных пакетов сообщений:

$T_{эт}$ – значений поля данных «Время жизни пакета»;

$O_{эт}$ – значений поля данных «Опции».

5. Определяют доверенные IP-адреса получателя и отправителя для запоминания этих значений в массивы $D_{эт}$, $I_{эт}$. Под доверенными IP-адресами понимают пары адресов, источника и назначения, легитимных абонентов различных фрагментов ИВС. Запоминают данные значения доверенных адресов получателя и отправителя пакетов сообщений в массив $D_{эт}$, $I_{эт}$.

6. Адаптируют информационно-вычислительную сеть (рис. 3). Под адаптацией понимается работа информационно-вычислительной сети в тестовом режиме для внедрения в конкретных условиях функционирования [3].

7. Измеряют реальные значения полей данных пакета «Время жизни пакета» и «Опции» для маршрута между j-ой парой доверенных адресов получателя и отправителя пакетов сообщений, где j=1, 2,..N , N – количество пар адресов доверенных абонентов. При

передачи пакетов по сети промежуточные узлы (маршрутизаторы) осуществляют их маршрутизацию по адресной информации, имеющейся в заголовке пакета [4].

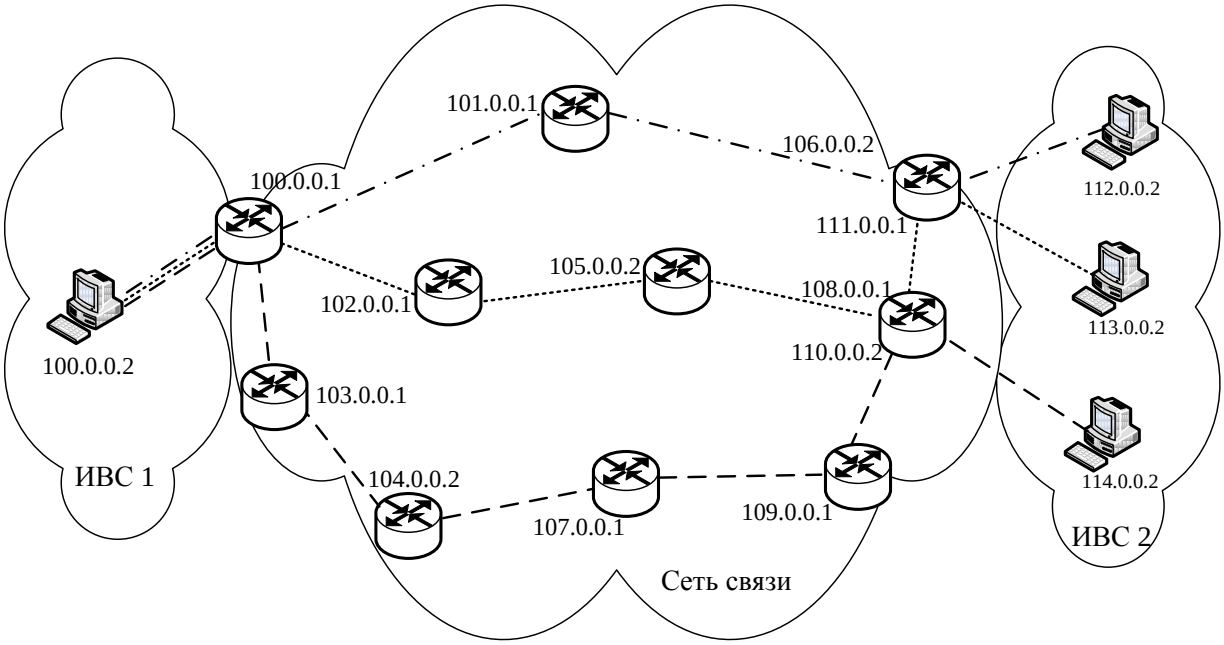

Рисунок 3 - Схема формирования маршрута передачи пакетов сообщений в ИВС

Таким образом, после передачи пакета по сети от источника к получателю сообщения, по определенному маршруту, адреса источника и получателя (поля «IP адрес назначения», «IP адрес источника»), количество пройденных маршрутизаторов (поле «время жизни пакета») и маршрут прохождения пакета (поле «опции») будут иметь одинаковые значение для всех пакетов сообщений, проходящих по этому маршруту. На рисунке 4 представлен пример значений полей данных IP пакета после прохождения по сети связи.

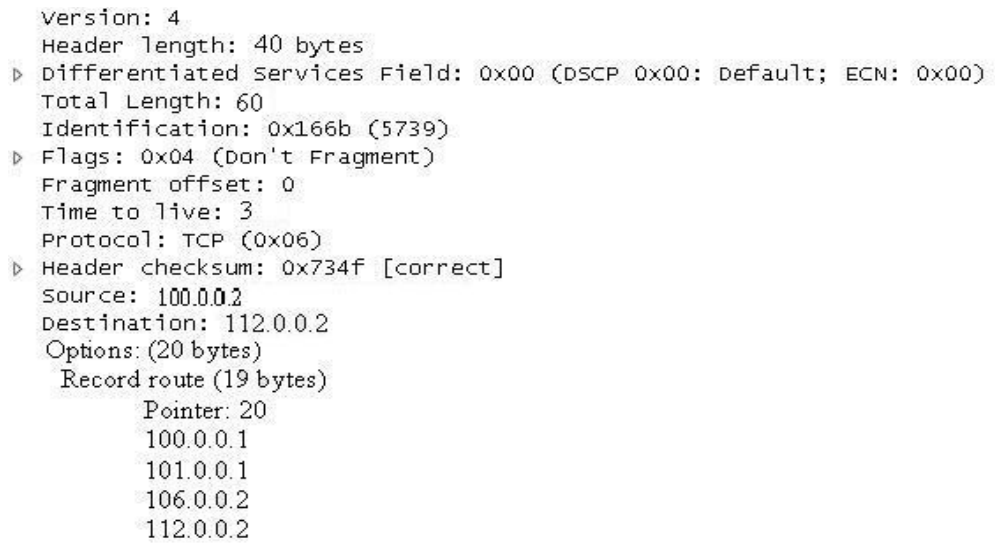

Рисунок 4 - Значения поля данных IP пакета после прохождения по сети связи

Эти значения запоминают в массивах $D_{эт}$, $I_{эт}$, $T_{эт}$, $O_{эт}$. Данную процедуру повторяют для всех пар доверенных адресов (j=N). Формируют таблицу 1, эталонных значений.

Таблица1

Эталонные значения полей данных «IP адрес назначения», «IP адрес источника», «Время жизни пакета» и «Опции»

IP адрес источника	IP адрес назначения	Время жизни пакета	Опции «запись маршрута»
100.0.0.2	112.0.0.2	3	100.0.0.1 101.0.0.1 106.0.0.2 112.0.0.2
100.0.0.2	113.0.0.2	5	100.0.0.1 102.0.0.1 105.0.0.2 108.0.0.1 111.0.0.1 113.0.0.2
100.0.0.2	114.0.0.2	6	100.0.0.1 103.0.0.1 104.0.0.2 107.0.0.1 109.0.0.1 110.0.0.2 114.0.0.2

8. После того как все эталонные значения проверяемых параметров собраны и записаны в соответствующие массивы, осуществляют перевод информационной вычислительной сети в режим реальной работы (эксплуатация).

9. Принимают *i*-й пакет сообщения из канала связи, где *i*=1, 2, 3,….

10. Запоминают *i*-й пакет сообщения в массив *P* для дальнейшей работы с заголовком *i*-го пакета.

11. Выделяют из заголовка *i*-го пакета значения поля данных «Время жизни пакета» T_i, поля данных «Опции» O_i , поля данных «IP адрес назначения» D_i и поля данных «IP адрес источника» I_i.

12. Запоминают в массивы *T, O, D, I* значения поля данных «Время жизни пакета» T_i, поля данных «Опции» O_i , поля данных «IP адрес назначения» D_i и поля данных «IP адрес источника» I_i.

13. Для выявления и блокирования компьютерных атак осуществляют поиск в массивах $D_{эт}$, $I_{эт}$ соответствующих значений полей данных «IP адрес назначения» D_i и «IP адрес источника» I_i полученного *i*-го пакета. При совпадении данных полей проверяют соответствие значений полей данных «Время жизни пакета» T_i и «Опции» O_i принятого пакета сообщений с эталонными значениями $T_{эт}$, $O_{эт}$.

14. Передают *i*-й пакет сообщения в информационно-вычислительную сеть при совпадении эталонных значений полей данных «Время жизни пакета», «Опции», «IP адрес назначения» и «IP адрес источника» со значениями полей данных из полученного пакета.

15. Принимают решение о подготовке атаки при несовпадении эталонных значений полей данных «Время жизни пакета», «Опции», «IP адрес назначения» и «IP адрес источника» со значениями полей данных из полученного пакета и запрещают передачу *i*-й пакета сообщения в информационно-вычислительную сеть, а также удаляют все значения из массивов *T, O, D, I*.

16. Повторяют действия, начиная с приема очередного пакета сообщения из канала связи до сравнения эталонных значений полей данных со значениями полей данных вновь принятого пакета сообщения и затем принимают решение о факте наличия или отсутствия компьютерной атаки.

Возможность реализации сформулированного технического результата была проверена путем машинного моделирования. С помощью моделирования получена взаимосвязь значений времени распознавания $t_{обн}$ (обнаружения) компьютерной атаки от объема фрагментированного сообщения $V_{сооб}$.

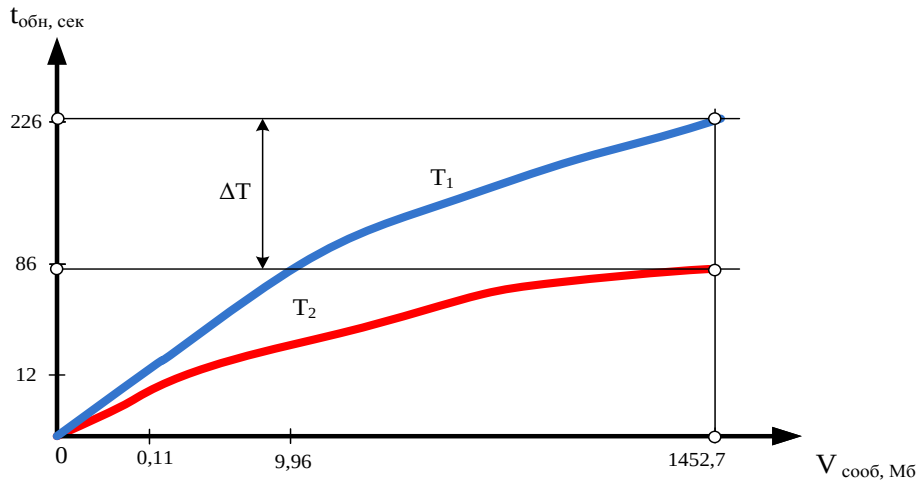

Рисунок 5 - Зависимость времени обнаружения компьютерной атаки от объема фрагментированного сообщения

На рисунке 5 представлена зависимость времени обнаружения компьютерной атаки от объема фрагментированного сообщения, для небольшого объема файла – 0,11 Мбайт, среднего объема файла – 9,96 Мбайт и большого объема файла – 1452,70 Мбайт с учетом того, что размер IP-пакета – 64Кб.

Достижение технического результата поясняется следующим образом. Для способа-прототипа при обнаружении компьютерной атаки осуществляется выявление фрагментированных пакетов за время T_1, которое зависит от объема передаваемого сообщения. Для предлагаемого способа выявление компьютерной атаки производится по результатам анализа каждого последовательно принятого пакета за время T_2, не ожидая времени необходимой для дефрагментации всего сообщения.

При этом разница в требуемом времени для обнаружения компьютерной атаки $\Delta T = T_1 - T_2$ тем больше чем больше объем фрагментированного сообщения, чем и достигается сформулированный технический результат при реализации заявленного способа, т.е. повышение оперативности обнаружения компьютерной атаки на информационно-вычислительную сеть.

Таким образом, заявленный способ за счет определения информации о подготовке компьютерной атаки путем использования трассировки маршрутов передачи пакетов по определенным доверенным маршрутам, поступающим в информационно-вычислительную сеть из каналов связи позволяет обеспечить повышение оперативности обнаружения компьютерной атаки на информационно-вычислительную сеть.

Библиографический список

1. 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.

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

3. ГОСТ Р 53622-2009. Информационные технологии. Информационно-вычислительные системы. Стадии и этапы жизненного цикла, виды и комплектность документов. М., 2009. 12 с.

4. ГОСТ Р ИСО/МЭК 7498-1-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. М., 1999. I, 62 с.

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, тел. 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: bobah_buch@mail.ru.

Стародубцев Юрий Иванович, профессор Военной академии связи им. Буденного, Заслуженный деятель науки РФ, д.в.н, профессор
Санкт-Петербург, Тихорецкий пр. д. 3, 194064; тел. (812) 556-93-41