УДК 621.372

СПОСОБ ЗАЩИТЫ ИНФОРМАЦИОННОЙ СЕТИ ОТ КОМПЬЮТЕРНЫХ АТАК

Динкилакер Виталий Викторович, Степанушкин Леонид Викторович, Павликов Сергей Николаевич, Коломеец Валерия Юрьевна
Владивостокского государственного университета экономики и сервиса,
Владивосток, *Россия.*
dinkilaker@gmail.com

Ключевые слова и словосочетания: способ, защита, компьютерная атака, угрозы

Аннотация: В работе приведен анализ угроз и методы защиты информационной сети от атак. Показан один из методов защиты. Приведена оценка эффективности.

METHOD OF PROTECTION AGAINST COMPUTER ATTACKS

Dinkilaker Vitaliy Viktorovich, Stepanuškin Leonid Viktorovichб
Pavlikov Sergej Nikolaevich, Valery Kolomeets Yurievna
Vladivostok state University of Economics and service
Russia. Vladivostok

Key words and word-combinations*: the way protection, computer attack threat.*

Abstract: in this paper is an analysis of threats and methods of protecting information networks against attacks. Shows one method of protection. See evaluation of effectiveness.

Значимость информационных технологий растет, степень угроз возрастает, поэтому актуальны исследования по оценке эффективности защиты как информации, так и сети в целом[1].

Известны способы защиты от компьютерных атак, приведенные и реализованные в патентах РФ [2], которые основаны на наблюдении за информационным потоком адресованных абоненту информационной вычислительной сети и включающее постоянно возобновляемый подсчет числа пакетов, выполняемый в пределах серии исследуемого интервала из канала связи, 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 [2, 3].

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 [2, 3].

Известны и другие способы оперативного динамического анализа состояний многопараметрического объекта [2, 3], позволяющих по изменению состояния элемента сети обнаруживать компьютерные атаки.

Анализ известных способов показывает пределы допусковой оценки разнородных динамических параметров в соответствующих информационных сигналах с обобщением по всему множеству параметров в заданном временном интервале и определяют относительную величину и характер изменения интегрального состояния многопараметрического элемента сети.

Недостатками указанных способов является узкая область применения, обусловленная тем, что, несмотря на возможность оперативной диагностики технического и функционального состояний многопараметрического элемента сети в нем применяют

ограниченную совокупность признакового пространства, что создает условия для пропуска удаленных компьютерных атак [4].

Анализ других способов защиты от компьютерных атак, приведённых в [4, 5] позволил определить основную проблему, которая определяется:

- низкой устойчивостью функционирования сетей в условиях воздействия компьютерных атак;
- отсутствием адаптационного механизма.

Применение процедур сравнения пакетов сообщений распознает только одно семейство компьютерных атак - "шторм" ложных запросов на установление соединения, тогда как компьютерные атаки других типов, обладающие высокими деструктивными возможностями, не распознаются [4 - 5].

Предлагается использовать большее количество пакетов и расширить пространство контролируемых параметры для сравнения принятых фрагментированных пакетов и по результатам сравнения принимать решение о факте наличия или отсутствия компьютерной атаки.

Объектом исследования является вычислительная сеть.

Предметом – методы защиты.

Целью работы является поиск технических решений по повышению достоверности обнаружения компьютерных атак на информационно-вычислительную сеть 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.

Новая совокупность существенных признаков позволяет достичь указанного технического результата.

Существующие угрозы безопасности информации могут быть реализованы путем использования протоколов межсетевого взаимодействия при построении распределенной сети, состоящей из нескольких сегментов, которые взаимодействуют через внешнюю сеть.
При этом угрозы могут быть реализованы путем проведения активных, пассивных или комбинированных атак, представляющих наибольшую угрозу. Считается, что потенциально опасны пассивные компьютерные атаки, которые не оказывается непосредственное влияние на работу сети, но при этом могут нарушать установленные правила разграничения доступа к данным или сетевым ресурсам.

В работе предложена модификация базовой модель угроз и обоснован выбор процедур эшелонированной системы обнаружения с прогнозируемыми вариантами развития событий с указанием контрольных точек и перечнем методов реагирования. Таким образом предложен усовершенствованный принцип трассировки маршрута прохождения пакетов с оценкой степени уязвимости и перечнем мер реагирования.

Список использованных источников:

1. Руководящий документ. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. ФСТЭК России. 2008.
2. Патент №2179738 «Способ обнаружения удаленных атак в компьютерной сети», класс G06F 12/14, заявл. 24.04.2000.
3. Патент РФ №2134897, опубликован 20.08.1999
4. Медведовский И.Д. и др. Атака на Internet. - М.: ДМК, 1999.
5. «Устройство поиска информации», патенту РФ №2219577 класс G06F 17/40, опубликован 24.04.2002
6.