ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ BDS-ТЕСТУВАННЯ ПРИ ДЕТЕКТУВАННІ СЛІДІВ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Семенов С.Г., Мовчан О.В.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Проведені дослідження показали можливість використання BDS-тестування при детектуванні слідів шкідливого програмного забезпечення.

В докладі наведено результати порівняльного аналізу методу детектування слідів шкідливого програмного забезпечення в мережевому трафіку. У табл. 1. приведені результати такого порівняння.

Таблиця – Результати порівняння розробленого методу з відомим кореляційним методом ідентифікації

Вид інформаційного трафіку	Кількість відліків			
	100	1000	5000	10000
HTTP-трафік	1,35	1,43	1,54	1,64
FTP-трафік	1,80	1,99	1,63	2,17
YouTube (720p)	1,60	1,68	1,85	2,23
YouTube (360p)	1,05	1,24	1,44	1,57
Skype (voice)	1,32	1,39	1,48	1,60
Skype (video)	1,13	1,20	1,32	1,58
E-mail	1,38	1,47	1,58	1,69

Як видно з табл., в усьому діапазоні вибраних «відрізків» експериментальних даних і для усіх видів інтерактивних служб спостерігається стійке підвищення ймовірності правильного детектування слідів шкідливого програмного забезпечення за допомогою процедур BDS-тестування. Так для FTP-трафіку ймовірність правильного детектування збільшується до 2,17 разів, для YouTube (720p) до 2,23 разів, для E-mail до 1,69 разів, для HTTP-трафіку до 1,64 разу і т.і.

Для вирішення завдання детектування окремих служб і сервісів по спостережуваному мережевому трафіку використаний апарат оцінки значущості розбіжностей двох і більше вибірок незалежних спостережень мережевого трафіку (критерій Вилькоксона) [1]. Він дозволяє із заданою точністю і достовірністю встановити приналежність різних потоків даних однієї і тієї ж генеральної сукупності. Це положення рекомендується використати в якості одного з елементів системи моніторингу мережевої активності, тобто на основі використання критерію Вилькоксона пропонується робити первинне детектування мережної служби або сервісу.

Література:

1. Семенов С.Г. Модели и методы распределения доступа и защиты данных в компьютеризированных информационно-измерительных управляючих системах критического применения / С.Г. Семенов. – Х.: НТУ «ХПИ». – 2013. – 360 с.