ПРИМЕНЕНИЕ ДИСКРЕТНОГО ВЕЙВЛЕТ-АНАЛИЗА В ИССЛЕДОВАНИИ ДИНАМИКИ ФИШИНГ АТАК

Дейнеко Ж.В.

Харьковский национальный университет радиоэлектроники

Переход к новым технологиям и расширение возможностей беспроводной передачи данных делает Internet неотъемлемым атрибутом повседневной жизни. Однако при этом приходится считаться с безопасностью передачи и получения различных данных, которые могут сопровождаться присутствием вредоносных компонент в передаваемом контенте. Фишинг атака является одной из разновидностей такого вредоносного компонента и в последнее время находит широкое распространение в информационном поле современных удаленных систем связи [1, 2].

В работе рассмотрена возможность и показана целесообразность проведения исследования фишинг атак с применением методологии дискретного вейвлет-анализа.

Целью данной работы является изучение динамики появления фишинг атак, выявление возможных закономерностей и разработка эффективных методов их предупреждения.

С точки зрения исследования динамики фишинг атак, имеются данные, которые характеризуют ежедневное количество фишинг атак. Такие данные позволяют судить о мощности фишинг атак в их ежедневном пересчете на протяжении некоторого периода времени, об интенсивности таких атак в определенные интервалы, либо их равномерности. При этом такие выводы могут быть полезны как для их предупреждения, так и для прогнозирования возможного роста фишинг атак.

Обработка и анализ последовательности данных, представленных в виде временного ряда, является одной из распространенных методологий в изучении различных процессов и явлений, относящихся к разным сферам деятельности и исследований. При этом многие временные ряды, порождаемые информационными потоками, обладают фрактальными свойствами и могут рассматриваться как стохастические фракталы. Выявление и изучение таких фрактальных свойств может быть осуществлено на основе методологии вейвлет-анализа [1].

Выделенные вейвлет-коэффициенты позволяют локализовать места неоднородностей и перепадов анализируемых временных рядов, то есть провести их пространственное разделение на области с характерными особенностями [2].

Для исследования динамики фишинг атак в качестве исходных данных были взяты данные с сайта http://www.phishtank.com, где представлены данные о подтвержденных фишинг атаках (рис. 1) и данные об общем количестве атак, представленных как фишинг атаки. Эти данные охватывают период с 1 октября 2006 года по 31 мая 2014 года в их ежедневном представлении. На рис. 1 и рис. 2 вдоль оси абсцисс отложены дни исследуемого периода времени, а вдоль

оси ординат – число подтвержденных и представленных фишинг атак соответственно.

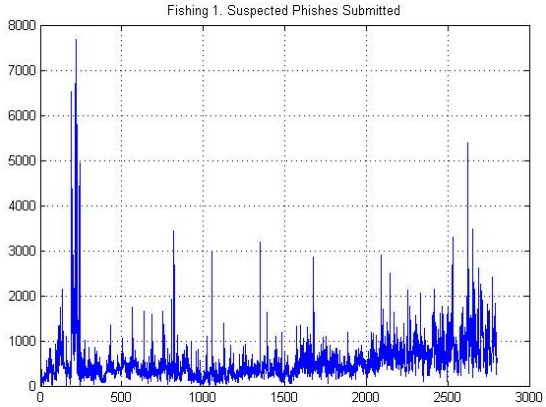

Рис 1. - Данные о подтвержденных фишинг атаках

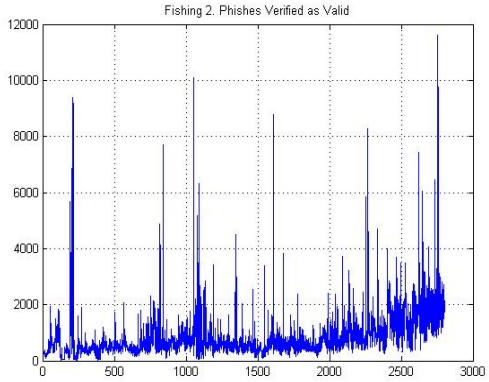

Рис 2. – Данные об общем количестве фишинг атак

В ходе исследования были построены графики автокорреляционных функций временных рядов. В обоих случаях наблюдается процесс медленно убывающей автокорреляционной функции. Следовательно, можно считать, что рассматриваемая динамика количества фишинг атак является самоподобным процессом [2]. В работе были рассмотрены общие положения, касающиеся вейвлет-анализа временных рядов, показаны особенности использования основных характеристик вейвлет-анализа для исследования временных рядов.

На основании реальных данных, которые характеризуются представленными временными рядами, рассмотрена идеология применения вейвлет анализа в исследовании фишинг атак. В частности показано, что исследуемым рядам данных свойственно наличие существенной длительности долгосрочной зависимости. Это говорит о наличии долгосрочной памяти в исследуемых рядах данных, что позволяет строить адекватные прогнозные модели по таким данным.

Анализ спектра вейвлет-энергии позволяет судить о наличии трендовой составляющей в структуре исследуемых рядов данных, что также может быть использовано для обоснования прогнозов относительно возникновения фишинг атак. В то же время взаимное исследование спектра вейвлет-энергии рядов данных, позволяет делать выводы о соответствии применяемых методов для идентификации многообразия различных событий, происходящих в среде Интернет, с точки зрения выявления потенциальных фишинг атак.

1. Deineko, Zh. Properties of wavelet coefficients of self-similar time series , V. Lyashenko, Zh. Deineko, M. Ahmad // International Journal of Scientific and Engineering Research. – 2015. – 6 (1). – P. 1492-1499.

2. Кириченко, Л.О. Анализ самоподобных и мультифрактальных свойств временных рядов, основанный на дискретном вейвлет-преобразовании / Л.О. Кириченко, Ж.В. Дейнеко // Радиоэлектроника и информатика. – 2011. – № 3. – С. 69–74.