СИСТЕМА ФИЛЬТРАЦИИ ФИШИНГОВЫХ ПИСЕМ

М.Н. Бычек, Т.В. Борботько

За последние 10 лет появилось множество разновидностей фишинга: фишинг с использованием SMS сообщений – смишинг, голосовой фишинг – вишинг, фишинг беспроводных сетей и др. Самым распространенным все еще остается фишинг с использованием электронной почты. По данными Statista, мировая база пользователей электронной почты достигла 3,9 миллиарда в 2019 году и, как ожидается, достигнет 4,3 миллиарда к 2023 г. Согласно отчету PhishMe research, 91 % кибератак производится с помощью фишинговых электронных писем, причем главными причинами, по которым люди обманываются фишинговыми письмами, являются любопытство (13,7 %), страх (13,4 %) и срочность (13,2 %) [1].

Система фильтрации фишинговых писем включает два подхода:

1. Информирование пользователей о наиболее заметных признаках фишинговых писем, таких, как:

- орфография и грамматика (грамматические и орфографические ошибки – две наиболее распространенные особенности фишинговых писем);
- общее приветствие или поздравление (поскольку фишинговые электронные письма отправляются случайным пользователям, нарушитель не обращается к получателям по имени – особенно, если электронное письмо содержит информацию об учетной записи или другую конфиденциальную информацию);
- вложения с гиперссылками, причем гиперссылка отличается от реальной ссылки [2].

2. Анализ входящей электронной почты программными средствами. В этом случае система анализирует заголовок, тело письма, содержащиеся ссылки и вложения. В частности, ссылки проверяются по множеству признаков, среди которых:

- наличие в ссылке IP-адреса;
- использование в ссылке символа @;
- использование шестнадцатеричных кодов символов;
- количество поддоменов в ссылке;
- возраст связанных доменных имен и др.

Вложения могут быть любого формата. Наиболее опасными являются файлы с расширениями *.bat, *.exe, *.zip, наиболее распространенными – *.xls, *.docx, *.pdf. наличие файлов такого типа является косвенным признаком фишинга. Кроме того, выполняется анализ тела письма на наличие JavaScript или HTML кода.

Литература

1. Sonowal G. Phishing and Communication Channels. A Guide to Identifying and Mitigating Phishing Attacks. Apress, 2022. 230 p.

2. Analysis of phishing emails / L. Burita [et al.] // AIMS Electronics and Electrical Engineering. 2021. Vol. 5, iss. 1. P. 93–116.