УДК 004.492.4

АВТОМАТИЗИРОВАННАЯ СИСТЕМА ПО ПРОТИВОДЕЙСТВИЮ ФИШИНГУ

Д. В. Лахмаков (МГУ имени А. А. Кулешова)
Науч. рук. ***И. Н. Сидоренко***,
канд. физ.-мат. наук

В современном цифровом обществе, где информация играет ключевую роль, обеспечение кибербезопасности становится неотъемлемой частью нашей повседневной жизни и деловой сферы. Основные принципы кибербезопасности, такие как конфиденциальность, целостность и доступность данных, являются фундаментом надежной защиты [1].

В Республике Беларусь за последние годы наблюдается значительный рост киберпреступлений, среди которых особую угрозу представляет фишинг. Фишинг можно охарактеризовать как метод манипуляции, при котором злоумышленники создают поддельные веб-сайты или рассылки [2], направленные на получение конфиденциальных данных пользователей (логинов, паролей, данных банковских карт) путем обмана. Злоумышленники применяют различные методы, включая фальшивые электронные письма, поддельные веб-сайты и вредоносные программные обеспечения.

В связи с этим возникает острая необходимость в разработке автоматизированной системы по противодействию фишингу, которая позволит эффективно выявлять угрозы и предотвращать утечку данных.

В рамках исследования была разработана концепция автоматизированной системы по противодействию фишингу, включающая:

- анализ входящих сообщений и веб-ресурсов;
- фильтрацию подозрительных ссылок и их блокировку;
- интеграцию с базами данных известных фишинговых сайтов;
- автоматическое уведомление пользователей о потенциальных угрозах.

Таким образом, внедрение автоматизированной системы по противодействию фишингу позволит значительно снизить количество успешных атак, повысить уровень кибербезопасности пользователей и минимизировать финансовые потери от интернет-мошенничества.

Литература

1. **Баланов, А. Н.** Кибербезопасность: учебник для вузов / А. Н. Баланов. – Москва: ЛитРес, 2021.
2. **Демиденко, А. Ю.** Кибербезопасность: как защитить свои данные /А.Ю. Демиденко. – Москва: 2022.