УДК 004.78(043.2)

**Парасочка Д.О.**

*Національний авіаційний університет,**Київ*

**БАГАТОРІВНЕВА СИСТЕМА АУТЕНТИФІКАЦІЇ ЗАСОБАМИ PHP**

З розвитком сучасних інформаційних технологій людина намагається підвищити свій рівень безпеки в інтернеті. Більшість сайтів, що нас оточує (форуми, інтернет-магазини, соціальні мережі…) використовує реєстрацію і подальшу авторизацію користувачів. Можна навіть сказати, що це майже необхідна функція кожного сайту. Тому в моїй доповіді увага буде зосереджена насамперед на системі авторизації.

При реєстрації нового користувача в базу данних необхідно записувати логін і пароль в подвійному md5 шифруванні.

При авторизації порівнюється логін і пароль і якщо вони вірні, то генерується випадковий рядок, який хешується і додається в БД. Також записується IP адреса користувача. В cookie ми записуємо його унікальний ідентифікатор і сгенерований хеш.

Перед нами може постати питання чому потрібно зберігати в cookie хеш випадково сгенерованого рядка, а не хеш пароля. Відповідь заключається в тому, що:

1. Із-за неуважності програміста, в системі можуть бути дірки і скористувавшись цими дірками зловмисник може викрасти хеш пароля з БД. В нашому випадку подвійне хешування пароля не допоможе хакеру, так як розшифрувати його він не зможе (теоретично це можливо, але на це він може витратити не один місяць, а може навіть і рік), а скористуватись цим хешем йому не вдасться, адже у нас при авторизації свій унікальний хеш прікріплений до IP користувача.

2. Якщо зловмисник за допомогою трояна витягне у користувача унікальний хеш, то скористуватись ним він також не зможе(якщо тільки користувач не вирішить знехтувати своєю безпекою и вимкне прив’язку до IP при авторизації).

Для того, щоб захистити форму логіна от перебору, можна використати капчу.

Отже, ці зміни в багаторівневій системі аутентифікації значно підвищать рівень безпеки користувачів багатьох сайтів.

*Науковий керівник – Артамонов Є.Б., к.т.н.*