

УДК 004.4

Маслов М.Г.<sup>1</sup>, Зайко Т.А.<sup>2</sup>

<sup>1</sup> студ. гр. КНТ-122м НУ «Запорізька політехніка»

<sup>2</sup> канд. техн. наук, доц. НУ «Запорізька політехніка»

## **ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ МЕТОДІВ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ**

Об'єкт дослідження – реалізація систем криптографічного захисту та методів авторизації на комерційному вебсайті в сучасних умовах.

Предмет дослідження – криптографічне шифрування та розшифровування даних, впровадження інноваційного методу авторизації на комерційному вебсайті за допомогою одноразових паролів (OTP) в сучасних умовах використання інтернет-ресурсів.

Мета роботи – дослідження та реалізація на практиці методів захисту даних та кондиційної інформації, в сучасних умовах, за допомогою криптографічного шифрування інформації.

Матеріали, методи та технічні засоби: мови програмування JavaScript, Python, середовище розробки та редагування програмного забезпечення Microsoft Visual Studio 2016 та середовище розробки PyCharm community Edition, методи структурного та об'єктно-орієнтоване програмування, а також програмне забезпечення багатфункціональний графічний редактор

Adobe Photoshop та графічний редактор Affinity Designer. Персональний комп'ютер, що функціонує на базі операційної системи Microsoft Windows 10 та з додатковим окремим використанням Ubuntu Server для розгортання та базування сайту на цій платформі. З використанням таких технічних комплектуючих персонального комп'ютера як, процесором Intel Core i3 10100, оперативною пам'яттю DDR4 з об'ємом 16 Гігабайтів, записним пристроєм тип SSD NVMe та периферійними пристроями: монітор з діагоналлю 19'', клавіатурою, координаційний пристрій типу «миша», вебкамерою та гарнітуром.

У ході дослідження були детально розглянуті історичні методи захисту інформації, а також сучасні методи шифрування, включаючи їхній розвиток та взаємозалежність. В результаті проведеного аналізу сформовано класифікацію криптографічних шифрів та виявлено ключові тенденції в розвитку сучасної криптографії та криптології.

Окрім теоретичних висновків, робота включає в себе практичний аспект, а саме розробку сучасного комерційного сайту. Під час його створення були використані передові методи та засоби шифрування даних, такі як протоколи SSL та TLS, що сприяють ефективному захисту інформації в онлайн-середовищі.

Галузь використання – інтернет-магазини, зорієнтовані на забезпечення високого рівня безпеки та оптимізації функціоналу для ефективної роботи в галузі електронної комерції (E-commerce).