UDC 004.056.5 (043.2)

Bohdan OLISHEVSKYI
National Aviation University, Kyiv

DEVELOPMENT OF IDENTIFICATION TECHNOLOGIES

During the times, there has been a need for personal identification. In the historical context, personal identification became particularly relevant with the emergence of formal systems of law, administration and governance. People nowadays prove their identity with their own documents, such as passport, driver's license, student ID card, etc.

With the advent of Internet technologies, many new methods of verifying and confirming identity have appeared. One of the key tasks of the identification and verification procedure is to ensure the security and protection of users' personal data.

In the early days of the Internet, email and passwords were the main ways to identify users. This method is considered to be one of the fundamental steps in the development of methods of personal identification in the online environment. It became widely used in the early days of the Internet and allowed users to create accounts on various websites and platforms.

The next breakthrough step was the disclosure of two-factor authentication. This method requires a user to provide exactly two verification factors to gain access to a website, application, or resource. Such method provides a higher level of security than single-factor authentication (SFA) methods, in which the user provides only one factor, usually a password or an access code.

What’s more, there are other methods of personal identification such as fingerprint and face recognition technologies that fall under the category of biometric security. A fingerprint scanner captures the fingerprint, converting the physical pattern into a digital format. After that, it confirms person's identity by comparing their fingerprints with previously recorded samples. In the case of facial recognition, the system scans the user's face and then special algorithms check for unique facial features. The device then identifies the user and allows access to the device if the face matches the one already registered in the system.

These technologies are mostly used for security and law enforcement, though there is increasing interest in other areas of use. Various phones, including the most recent iPhones, use face recognition to unlock the device. The technology offers a powerful way to protect personal data and ensures that

sensitive data remains inaccessible if the phone is stolen. Beyond unlocking phones, facial recognition also works by matching the faces of people walking past special cameras, to images of people on a watch list.

Apart from the personal identification methods, there is also a validation of the user as a member of the human race. Such a protection measure was developed due to a need to protect web resources from automated attacks, such as spam, password brute force, and other forms of abuse. To accomplish these tasks, the CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) system was developed.

This test is designed to determine if an online user is really a human and not a bot. There are several different types of CAPTCHAs such as text, image and audio. CAPTCHAs provide challenges that are difficult for computers to perform but relatively easy for humans. For instance, identifying stretched letters or numbers, or clicking in a specific area. Once the user has completed the test, the system knows they're human and allows them to carry on with whatever they're doing on the web page.

To sum up, technologies of identity verification and identification are evolving and becoming more and more reliable. And even though there are such strong security methods as, for example, two-factor authentication, there are still hackers who are able to bypass these systems. That is why there is still a need to develop and implement new and effective techniques and methods to provide more reliable and effective protection.

Scientific supervisor: Nataliia DENYSENKO,
Senior Lecturer