

УДК 004.75:339.722

Івлєв В.Ю.¹, Воскобойник В.О.²

¹студ. гр. РТ-819 НУ «Запорізька політехніка»

²канд. техн. наук, проф. НУ «Запорізька політехніка»

ВРАЗЛИВІСТЬ МЕТОДІВ АУТЕНТИФІКАЦІЇ

Законодавство держави захищає своїх громадян від помилкових звинувачень відносно скоєння правопорушень. Приватні компанії, на жаль, можуть і далі продовжувати використовувати низький рівень досвідченості та розумінь систем аутентифікації в цілому.

Одним з шляхів вирішення цього питання є доцільним застосування алгоритмів розпізнавання осіб в межах комерційного використання світових брендів Microsoft, Google, Amazon і інших. Саме вони стають частиною сучасних методів інформаційної безпеки. Незалежно від платформ операційних систем чи інтерфейсу обміну інформаційними ресурсами, методи аутентифікації є і будуть важливими, а алгоритми яких постійно мають вдосконалюватися.

Аналіз показав, що досвід Японського національного інституту інформатики, який розробив окуляри з LED-лампами, які наче б то, висвітлюються з випромінюванням як білина, закриваючи обличчя від систем розпізнавання, підсвічуючи очі і ніс, скритні. Для людського ока вони майже непомітні. Розпізнавання особистості стає непомітним та не можливим на даний час.

Другим варіантом недосконалості аутентифікації з застосуванням біометрії є силіконова маска, яка надрукована на 3D-принтері. Камера, побачивши обличчя, розпізнає особу згідно даних в базі даних. Але це буде лише прообразом особи, яка не враховує приватні особливості.

Технології аутентифікації та їх застосування постійно вдосконалюються. Цьому прикладом є проект стартап Hyperface, згідно якому, винахідники вирішили виявити усереднені патерні з своїм зображенням. Вони, в завершенні своєї ідеї, надрукували свої зображення на тканині, що привело до «обману камер спостережень».

Не слід забувати про дактилоскопію як складову аутентифікації особи. Існує декілька способів виявлення та фіксації рельєфу на пальці людини.

Найчастіше використовується оптичний: візуальний малюнок при видимому світлі або відтиск на папері (тактильність).

Наведені підходи аутентифікації та можливості протидії їм на сьогодні є умовними, оскільки розвиток сучасних технологій постійно удосконалюються. Це свідчить про те, що існує можливість обману (чи обходу) систем аутентифікації.