мий при наборі».

22. Не використовуйте запропоновану системою можливість запам'ятати пароль під час його використання.

23. Необхідна періодична зміна паролю. Термін зміни паролю визначається адміністратором системи, але не рідше одного разу в 60–90 днів.

24. Зміна паролю повинна бути не за графіком, а випадковим чином.

25. Новий пароль повинен значно відрізнятися від попереднього.

26. Створений пароль необхідно запам'ятати (забороняється записувати та залишати пароль на видному місці).

27. Необхідно негайно змінювати пароль у разі підозри про його розкриття.

При вимаганні від користувачів створювати надійні паролі необхідно враховувати також те, що складні паролі можна легко забути, і їх з більшою ймовірністю будуть записувати на папері, що передбачає певний ризик. З іншого боку, якщо зажадати від користувачів запам'ятовувати паролі, то вони будуть придумувати більш легкі паролі, що серйозно збільшить ризик злому [5]. Необхідно також зазначити, що створення надійного паролю буде мати позитивний результат тільки при забезпеченні належного антивірусного захисту.

1. Концепція програми інформатизації Міністерства внутрішніх справ на 2018–2020 роки, затверджена рішенням колегії МВС від 05 лист. 2018 р. № 18км: Наказ МВС України від 11 груд. 2018 р. № 1004.

2. Про затвердження Положення про Єдину інформаційну систему МВС та переліку її пріоритетних інформаційних ресурсів: постанова Кабінету Міністрів України від 14 лист. 2018 р. *Урядовий кур'єр*. 2018. № 235. URL: https://zakon.rada.gov.ua/laws/show/1024-2018-%D0%BF.

3. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: наказ МВС України від 03 серп. 2017 р. № 676. *Офіційний вісник України*. 2017. № 75. Ст. 2306. Код акта 87310/2017. URL: https://zakon.rada.gov.ua/laws/show/z1059-17.

4. Про Національну поліцію: Закон України від 02 лип. 2015 р. № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19.

5. Кудінов В. А. До проблеми щодо створення надійних паролів користувачів Інтегрованої інформаційно-пошукової системи МВС України // Актуальні проблеми управління інформаційною безпекою держави: матеріали VIII наук.-практ. конф. (Київ, 24 трав. 2017 р.). Київ: Нац. акад. СБ України, 2017. С. 54–56.

Мирошниченко Володимир Олексійович
доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ,
кандидат технічних наук, доцент

БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ КЛІЄНТІВ У БАНКІВСЬКІЙ СФЕРІ

Поява нового покоління механізмів підтвердження особи здатна змінити уявлення про багато речей, до яких ми звикли і користуємося практично щодня. Йдеться про біометричну ідентифікацію особи. Біометрія включає в себе кілька різних технологій, які з певних вимірюваних характеристик з високою часткою ймовірності ідентифікують конкретну людину. До таких технологій належать фото- та відеосистеми розпізнавання осіб, голосів, підписів, відбитків пальців і деякі інші [1].

Всі вони можуть застосовуватися комплексно або окремо і зараз в основному є додатковим чинником безпеки у банківській галузі. Традиційні способи підтвердження особи, такі як паспорт, підпис і фотографія, застосовуються давно, і навряд чи від них скоро відмовляться. Вони уніфіковані і визнані в усьому світі. Інша річ, що з розвитком технологій і високим ступенем проникнення в наше життя електронних сервісів та пристроїв відбувається закономірне переформатування деяких видів послуг.

Активний розвиток онлайн-торгівлі, поширення пластикових карт як інструментів оплати зажадали нових способів ідентифікації особи при здійсненні платежів. І вони не змусили себе чекати. З'явилися ПІН-коди банківських карт, паролі в інтернет-банкінгу та підтверджуючі одноразові SMS-повідомлення. Темп нашого життя прискорюється, і застосування нових технологічних рішень в банківській сфері є дуже затребуваним: час транзакції стає ключовим параметром при оплаті товарів і послуг. Разом з тим необхідно зберігати високий рівень забезпечення безпеки грошових переказів. І тенденція така, що банки все активніше починають впроваджувати біометрію як додатковий спосіб ідентифікації клієнта при проведенні платежів. Світовий досвід показує, що мультибіометрія (розпізнавання особи відразу за кількома індивідуальними характеристиками – за обличчям, голосом або відбитками пальців)

можлива при використанні смартфона як терміналу, через який підтверджується транзакція. При цьому зберігається і звична електронна аутентифікація (SMS-підтвердження). Наприклад, найбільші платіжні системи VISA і MasterCard спільно з найбільшими банками нещодавно запустили механізм сканування відбитку пальця для підтвердження платежу на касових терміналах, що є прикладом подвійної ідентифікації клієнта. Запуск такого сервісу дуже добре ілюструє сучасний рівень готовності банківської сфери до впровадження технологій біометричної ідентифікації, можливостей таких систем і те, в якому напрямку вони будуть розвиватися. Участь у проекті серйозних компаній, таких як Visa і MasterCard, говорить про високу надійність самої технології, яка за рівнем захисту не поступається ПІН-коду.

Персональна інформація має високий ступінь захисту завдяки тому, що біометричні дані клієнтів, отримані з POS-терміналу, обладнаного сканером, відразу перетворюються в унікальний числовий код. Цей код прив'язується до зареєстрованої банківської картки, а для підтвердження транзакції достатньо піднести палець до сканера свого смартфона. Таким чином, самі біометричні дані нікуди не передаються, відповідно, перехопити їх неможливо. Обмежити широке впровадження біометричного розпізнавання за відбитком пальця можуть суб'єктивні чинники: далеко не у кожного є смартфон зі сканером і спеціалізовані додатки для оплати. Це рішення – поки скоріше для найбільш «просунутих» користувачів, які прагнуть спробувати ноу-хау. Тому зараз досить складно розглядати дактилоскопію як оптимальний і єдиний спосіб біометричної ідентифікації в банківській сфері.

У багатьох ситуаціях використання біометричного розпізнавання за обличчям виглядає кращим, оскільки безконтактне достовірне розпізнавання за обличчям не залежить від того, є у людини смартфон зі сканером відбитків пальців, чи ні, якщо POS-термінал та банкомат обладнаний відеокамерою, значить є можливість розпізнати платника. Біометрію вигідно використовувати в комбінації з іншими способами ідентифікації особи без обмежень, оскільки плюси є очевидними: авторизація за біометричними характеристиками відбувається швидко, вона зручна і має високий ступінь захисту. Крім того, саме ідентифікацію за обличчям доцільно застосовувати не тільки для підтвердження платежів, а й у внутрішній роботі банку, наприклад при розгляді запиту на видачу кредиту.

Система біометричного розпізнавання осіб інтегрується з CRM-системою, де зберігається інформація про клієнтів, які будь-коли зверталися до кредитної установи. З її допомогою особа клієнта підтверджується практично миттєво. Операціоніст відразу отримує вичерпну інформацію про його кредитні історії і в режимі реального часу перевіряє інформацію про потенційного позичальника. Унікальні характеристики особи людини дозволяють безпомилково її ідентифікувати, завдяки чому біометричне розпізнавання осіб поступово впроваджується ще й як ефективний інструмент боротьби з кредитними шахраями [2].

Слід зазначити, що спосіб біометричної ідентифікації за обличчям – уніфікований. Його зручно використовувати і для авторизації працівника банку, коли він входить у внутрішні службові бази. Тут також можливою є комбінована ідентифікація: біометрія і/або пароль, або електронний ключ. Крім того, за допомогою системи біометричної ідентифікації за обличчям легко враховувати робочий час працівника.

Таким чином, одна технологія вирішує в банківському секторі відразу кілька завдань: забезпечує безпеку фінансових процесів, оптимізує внутрішні бізнес-процеси, підвищує якість обслуговування клієнтів та надає нові зручні сервіси. Методи розпізнавання людини за біометричними даними – відбитком пальця, голосом або обличчям – дуже перспективні в банківській сфері. Авторизація за допомогою біометричної ідентифікації стає все більш актуальною при здійсненні покупок через інтернет, вона здатна перевернути наше уявлення про онлайн-торгівлю. Можливо, ні CVV-код, ні самі пластикові карти через якийсь час нам просто не знадобляться в результаті активного впровадження можливостей аутентифікації у мобільних пристроях. Технології продовжують розвиватися, чітко простежується тенденція їх впровадження, але й традиційні способи ідентифікації особи поки що збережуться. Для широкого втілення біометричних технологій на всіх рівнях банківської системи необхідним є формування єдиної бази біометричних даних осіб, але сьогодні така база у необхідному обсязі поки що відсутня. Але прогнози говорять, що в перспективі п'яти-восьми років біометрична ідентифікація стане основним способом підтвердження особи при отриманні фінансових послуг. Поки ж будуть використовуватися в сукупності кілька способів ідентифікації особи одночасно.

1. Мирошниченко В.О. «Динамічний фоторобот» людини та перспективи його використання. *Протидія організованій злочинній діяльності*: матеріали Всеукраїнської наук.-практ. інтернет-конф., м. Одеса, 31 бер. 2017 р. Одеса, 2017. С. 103-105.

2. Мирошниченко В.О., Вишня О.В. Аналіз біометричних систем ідентифікації особи в умовах діяльності правоохоронних органів. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*: зб. наук. праць. 2007. № 1 (32). С. 314-321.