Режим доступу: http://zakon0.rada.gov.ua/laws/show/2456-17
2. Романенко О.Р. / Фінанси: Підручник. – К: Центр навчальної літератури, 2004. – 312 с.
3. Федосов В. Бюджетний менеджмент: Підручник / В. Федосов, В. Опарін, Л. Сафонова та ін.; За заг. ред. В. Федосова. — К.: КНЕУ, 2004. – 864 с.
4. Федосов В.М., Теорія фінансів: Підручник / За ред.. проф. В.М.Федосова, С.І. Юрія. – К.: Центр учбової літератури, 2010. – 576 с.
5. Юрій С.І. Фінанси: Підручник / За ред. С.І. Юрія, В.М. Федосова. — К.: Знання, 2008. – 611 с.
6. Сафонова Л.Д. «Ризики бюджетного фінансування в Україні: чинники та шляхи мінімізації» / Сафонова Л.Д., Степанюк Н.І., // Світ фінансів - 1(50). – 2017. - с.82-90.

Слатвінський М. А.
к.е.н., доцент, завідувач кафедри фінансів, обліку та економічної безпеки
Уманський державний педагогічний університет імені Павла Тичини
м. Умань, Україна

ЕКОНОМІКА БЕЗПЕКИ: ЗАХИСТ БАНКІВСЬКИХ ОПЕРАЦІЙ

Банківська система з все більшим застосуванням банками нових технологій в просуванні свої продуктів та послуг зіштовхується також із все більш розширюваним спектром потенційних небезпек, від комп'ютерних вірусів до шахрайства та організованої злочинності. Як наслідок, все більше уваги приковано до питань безпеки, що обумовлює невпинне зростання попиту на товари та послуги, пов’язані з безпекою.

Фактично, це породжує один із сегментів економіки безпеки, що не зважаючи на широкий спектр підходів до розуміння її сутності, розглядається далі як індустрія безпеки, що пов’язана з діяльністю із забезпечення безпеки банківських установ. Індустрія безпеки – це сукупність ряду підприємств та організацій, які надають продукти та послуги з безпеки, що включають як пожежні та охоронні сигналізації, замки, сейфи, так і системи електронного доступу та біометрії. Обсяги цього ринку складно піддати кількісному виміру, так як не всі заходи з безпеки пов’язані з витратами, однак окремі дані свідчать про щорічний темп приросту товарообігу у розмірі 7-8%, що перевищує середньорічні темпи економічного зростання.

Безпека банківських операцій користується значним інтересом в науковій літературі, оскільки змістовно пов’язана із сутністю банківського бізнесу та є складовою безпеки банку та його персоналу. Особливу увагу звертають на порушення діючих внутрішньобанківських порядків та правил, допущення чи вчинення дій у банку в особистих інтересах банківського персоналу чи його власників, а також в інтересах конкуруючих банківських та інших фінансово-кредитних установ, організованої злочинності і державних посадових осіб [1; 2; 3; 7]. Тоді як питання сучасних банківських технологій залишається малодослідженим в науковій літературі.

Серед банківських операцій значного поширення набув інтернет-банкінг,

що однак супроводжується зростанням банківського шахрайства поруч із розвитком електронних технологій, розширенням функціоналу платіжних карт і каналів дистанційного банківського обслуговування (ДБО). Виділимо такі основні ризики для користувачів інтернет-банкінгу, що однаково актуально для фізичних та юридичних осіб – користувачів банківських послуг: перехоплення паролів та логінів з клавіатури чи екрану комп'ютера, фішинг, шкідливе програмне забезпечення, отримання віддаленого доступу до комп'ютера користувача банківських послуг, перехоплення смс, дублювання сім-карт, крадіжка ключа електронного цифрового підпису (ЕЦП), підміна транзакцій.

Проблеми насамперед стосуються недосконалих систем автентифікації користувачів – фізичних осіб (на основі смс-повідомлень), використання ЕЦП (отримання фізичного доступу до нього). В цьому напрямі розроблено нові додаткові технології захисту (алгоритми та технічні засоби), що свою чергу призводить до збільшення банківських витрат.

Окреме місце займають ситуації пов'язані з людським чинником – витоками інсайдерської інформації, що в тому числі може призводити до розкрадання коштів з рахунків клієнтів; погана ознайомленість більшості користувачів банківських послуг про сучасні та ефективні способи захисту – лише 5 % повністю ознайомлені з ними.

Згідно з даними дослідження проведеного компанією маркетингових і соціологічних досліджень «GfK Ukraine» на замовлення Української міжбанківської асоціації членів платіжних систем ЄМА [6], 11% користувачів платіжними картками не змогли назвати жодного способу захисту, а інші респонденти зазначили, що їм відомі всього 1-2 способи захисту від шахрайства. При цьому основні названі способи захисту були традиційними: 52% опитаних знають про необхідність не повідомляти нікому ПІН-код картки; 22% – не передавати карту іншим людям; 14% – не зберігати ПІН-код разом з картою, у тому числі, не писати його на карті (рис. 1).

Шляхом до вирішення існуючих проблем із захистом банківських операцій є розвиток та використання новітніх технологій на основі біометрії, що вже почали займати свою частку на ринку.

Під біометрією розуміємо технологію ідентифікації особи, яка використовує фізіологічні параметри суб'єкта (код ДНК, відбитки пальців, райдужну оболонку ока, зображення обличчя, тембр голосу) для ідентифікації [4, с. 54-55].

Зокрема, фахівці з компанії Socure (Нью-Йорк, США) розробили програму Perceive, що використовує біометричні параметри для авторизації (фото зроблене клієнтом на смартфон з додатковою перевіркою його за профілями в соціальних мережах. Цю технологію в рамках боротьби з шахрайством по розрахунках з використанням пластикових карток вже використовують декілька американських банків. Якщо банк USAA використовує для ідентифікації через окремий мобільний додаток зображення обличчя, то Wells Fargo – зображення очей клієнта.

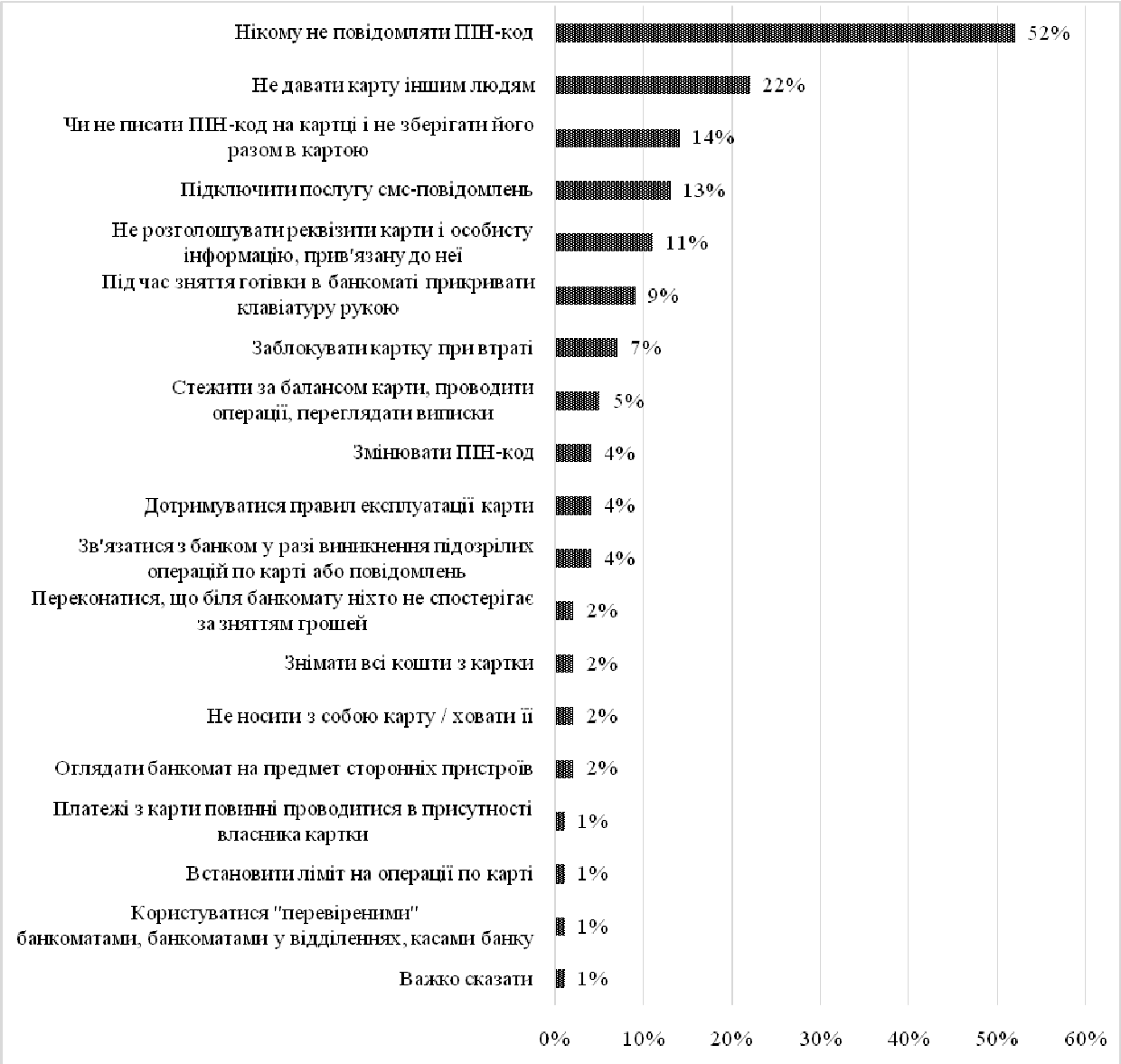

Рис. 1 - Інформованість про засоби захисту від шахрайства у сфері платіжних карт

**За даними GfK Ukraine [6]*

Британський банк Halifax випробував нову систему ідентифікації своїх клієнтів за допомогою моніторингу серцебиття з використанням спеціального браслета, що дозволяє клієнтам отримувати доступ до свого рахунку без введення додаткових кодів і паролів.

MasterCard протестував систему використання відбитків пальців для підтвердження онлайн-платежів (в окремих країнах Європи і в США). В Україні, наприклад «Приватбанк», також успішно використовується ідентифікація клієнта на основі відбитку його пальця в додатку Privat24.

Разом з тим, безпека ідентифікації за відбитком пальця була скомпрометована однією із перших дослідницькою компанією SRLabs, яка легко обійшла сканер відбитків пальців смартфона, використовуючи копію відбитка пальця і тонер.

Отже, існуючі біометричні технології захисту, будучи перспективними,

поки ще не позбавлені своїх недоліків, що не сприяє остаточному вирішенню проблеми.

Системи біометричної ідентифікації користувачів банківських послуг виводять на новий рівень інформаційну безпеку. Для банківської системи запровадження біометричних даних, як засобу ідентифікації, стане форпостом формування цілісної банківської системи захисту. Вони значно поширені в багатьох сферах, де необхідна регламентація доступу до конфіденційної інформації, матеріальних цінностей, приміщень чи територій тощо. Біометричні технології широко використовуються в області безпеки банківських операцій, інвестування та інших фінансових траназакцій, а також роздрібній торгівлі, охороні правопорядку, сфері охорони здоров'я, останнім часом активно використовуються у сфері соціальних послуг [5, с. 145]. В найближчій перспективі біометричні технології, за відсутності поки що кращих аналогів, будуть відігравати провідну роль в багатьох сферах персональної ідентифікації, з окремим використанням чи поруч з іншими інструментами.

Найпоширенішими біометричними параметрами, які апробовані в системах персональної ідентифікації, на даний час є: відбитки пальців, райдужна оболонка ока, зображення обличчя.

Отже, швидке зростання частки використання інформаційних технологій при здійсненні банківських операцій обумовлює виникнення додаткової уваги до додаткових технологій захисту інформації. Переважна більшість систем захисту інформації орієнтовані на використання біометричних ознак. Застосування біометричних ознак для захисту банківських операцій в Україні дасть потужний розвиток системі безпеки банківського сектору. А це, в свою чергу, призведе до мінімізації різного роду ризиків для банківських клієнтів та банків загалом, зокрема, після роботи з удосконалення використовуваних алгоритмів. що убезпечить від використання обхідних шляхів при автентифікації клієнта банку.

Література:

1. Букин С. Безопасность банка [Электронный ресурс] / С. Букин // Банковские технологии. – 2003. – № 9. – Режим доступа: www.bizcom.ru/security/2003-09/01.html
2. Гриценко Р. Економічна безпека банківської системи України // Вісник Національного банку України. – 2003. – № 4. – С. 27-28.
3. Зубок М. І. Безпека банківської діяльності : навч. посібник / М.І. Зубок. – К.: КНЕУ, 2002. – 190 с.
4. Лисенко А. М. Застосування біометричних систем для ідентифікації особи / А. М. Лисенко // Вісник Київського нац. ун.-ту ім. Т.Шевченка. Юридичні науки. – 2004. – № 60/62. – С. 87-91.
5. Чередниченко В.Б. Біометричні методи у системах захисту інформації / В.Б. Чередниченко, К.Е. Чередниченко// Системи обробки інформації. – 2012. – Вип. 4(1). – С. 145-148.
6. «Шахрайство та грамотність у сфері використання платіжних інструментів: погляд українського споживача». GfK Ukraine за замовленням Української міжбанківської Асоціації членів платіжних систем «ЄМА» від 18.03.2014 р. [Електронний ресурс] – Режим доступу: http://www.gfk.com/ua/news-and-events/press-room/pressreleases/Pages/ema_research_release.aspx.