найкращий спосіб вберегтися від інфляції – купувати іноземну валюту.

Отже, фінансова поведінка вітчизняних домогосподарств є складним як економічним, так і соціальним явищем. Її формування та характерні особливості залежать від багатьох факторів і мотивів, а результат цієї поведінки впливає на розвиток ринку фінансових послуг. Вважаємо, що вирішення окреслених проблем сприятиме активізації фінансової поведінки вітчизняних домогосподарств і залученню їх до діяльності на фінансовому ринку України

Список використаних інформаційних джерел

1. Дудинець Л. А. Фінансова поведінка домогосподарств та її детермінанти / Л. А. Дудинець, Г. Г. Голуб, Р. Р. Голуб // Соціально-економічні проблеми сучасного періоду України. – 2019. – Вип. 2. – С. 42–47.
2. Формування фінансової поведінки домогосподарств в Україні / В. М. Мельник, І. Д. Якушик, І. А. Ломачинська, О. О. Драган. – Херсон : ВД Гельветика, 2014. – 212 с.
3. Фінансова грамотність, обізнаність та інклюзія в Україні [Електронний ресурс] : звіт про дослідження. – 2017. – 69 с. – Режим доступу: https://bank.gov.ua/doccatalog/document?id=83136332. – Назва з екрана.

ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ ДІЯЛЬНОСТІ

Д. В. Пиріг, *студент спеціальності Фінанси, банківська справа та страхування, група ФКбі-21*

В. В. Карцева, *науковий керівник, д. е. н., професор, завідувач кафедри фінансів і банківської справи*

Вищий навчальний заклад Укоопспілки «Полтавський університет економіки і торгівлі»

Важлива роль у забезпеченні національної безпеки України, а особливо її економічної складової, належить процесам забезпечення інформаційної безпеки держави у банківському секторі. Сучасний банк важко уявити без ефективної автоматизованої інформаційної системи, разом з тим, саме вона є його найбільш уразливою стороною. Жоден сучасний банк не може обійтися без комп'ютерних систем, які в сучасних умовах є джерелом ви-

никнення ризиків і загроз, що обумовлено використанням нових інформаційних технологій.

Серед основних об'єктів інформаційної безпеки банківських установ виокремимо наступні: – фінансові ресурси – національна й іноземна валюта, банківські операції та угоди банку, кошторисності, фінансові документи; – персонал банку – керівництво і вищий менеджмент банку, особи, які мають доступ до конфіденційної інформації, банківської та комерційної таємниці, інші працівники банку; – матеріальні засоби – апаратні засоби інформаційних технологій, носії даних, будівлі, приміщення, меблі, транспорт тощо; – сервісні ресурси та підтримуюча інфраструктура – обслуговуючі засоби обчислювальної техніки, енергопостачання, забезпечення необхідних умов експлуатації і тощо; – програмне забезпечення – прикладне, системне чи сервісне програмне забезпечення тощо, яке використовується співробітниками банківської установи для роботи з системами і клієнтами; – інформаційні ресурси – будь-яка інформація банку, що обробляється та зберігається в банківській установі (бази даних, файли, документи) [2].

Фінансова глобалізація призвела до інформаційного буму. Вітчизняним злодіям стали відомі методи та механізми шахрайства, що були вигадані та успішно використовувались у багатьох країнах світу [1]

Швидкі темпи розвитку і поширення інформаційних технологій, загострення конкурентної боротьби тощо вимагає створення цілісної системи інформаційної безпеки. Формування інформаційної безпеки банківських установ та забезпечення ефективного захисту інформації є надзвичайно актуальним, оскільки щоденно обробляється великий обсяг інформації різного рівня конфіденційності.

Основним принципом інформаційної безпеки, якого доцільно дотримуватися банку, є підтримання таких властивостей інформації, як: конфіденційність – захист від несанкціонованого ознайомлення; цілісність – захист від несанкціонованого спотворення, руйнування або знищення; доступність – захист від несанкціонованого блокування.

Саме тому все більшого поширення набирають послуги IT outsourcing для банків з метою якнайшвидшого приведення ме-

тодів захисту їхніх інформаційних систем у відповідність до вимог НБУ. Насамперед, такі послуги пропонують ІТ-компанії, які проводять загальний технічний аудит та перевірку регламентного забезпечення функціонування систем захисту банку. Така перевірка має включати penetration test (тест на проникнення як метод оцінювання захищеності комп'ютерної системи), який допомагає виявити технічні недоліки інформаційних систем та визначити необхідний перелік потрібних систем безпеки [3].

Отже, інформаційна безпека банків вимагає комплексного, чітко спланованого, поетапного проекту вдосконалення систем її захисту. Такий комплекс має включати три основні підходи щодо виявлення загроз для функціонування інформаційних систем банку: технологічний – першочерговий аудит, впровадження оновлених методів захисту та подальша оптимізація всієї ІТ-інфраструктури банку з метою не лише позбутися недоліків, але й попередити їх у майбутньому; робота з персоналом та адміністрацією банку – на цьому етапі необхідно не лише перевірити належне регламентне забезпечення роботи інформаційних систем, але й провести подальші роз'яснювальні роботи з персоналом; з іншого боку, це робота з керівництвом банку, що має забезпечити розуміння всіх можливих ризиків наступних кібератак та санкцій НБУ за невідповідність вимог НБУ; правове забезпечення, яке дозволило б належним чином врегулювати відносини між банком та ІТ-компанією щодо конфіденційності інформації.

Кожній банківській установі доцільно розробити власну систему інформаційної безпеки та ефективно впроваджувати комплекс заходів із захисту конфіденційних даних та інформаційних процесів.

Список використаних інформаційних джерел

1. Зачосова Н. В. Формування системи економічної безпеки фінансових установ : монографія / Н. В. Зачосова. – Черкаси : ПП Чабаненко Ю. А. – Черкаси, 2016. – 375 с.
2. Зубок М. І. Безпека банківської діяльності : навч. посіб. / М. І. Зубок. – Київ : КНЕУ, 2002. – 190 с.
3. Павловська А. Кібербезпека у банківському секторі: чи допоможе ІТ – outsourcing? / А. Павловська, З. Халімон [Електронний ресурс]. – Режим доступу: https://www.sk.ua/sites/default/files/kiberbezpeka_u_bankivskomu_sektori.pdf. – Назва з екрана.