Оцінювання ризику атак соціальної інженерії в банківських установах

УДК 004.056.5 (336.71)

Дар'я Семидетнова[1], Ірина Вінковська[2], Дар'я Курінська[3]

Національний університет «Одеська політехніка», [1]9560456@stud.op.edu.ua, [2]vinkovska.i.s@op.edu.ua, [3]10252746@stud.op.edu.ua

В умовах сучасної цифровізації фінансових послуг соціальна інженерія залишається однією з найнебезпечніших загроз, оскільки спрямована не лише на технічні вразливості, а й на експлуатацію психологічних особливостей людини. Соціальна інженерія, що базується на маніпулюванні довірою, страхом або цікавістю співробітників, дозволяє зловмисникам отримувати доступ до конфіденційних даних, систем дистанційного банківського обслуговування та внутрішніх мереж. Враховуючи умови стресу та багатозадачності, в яких працюють працівники банківських установ, а також значні потенційні збитки від успішних атак, питання оцінювання рівня вразливості персоналу до методів соціальної інженерії набуває особливої актуальності [1].

Метою роботи є дослідження та оцінювання рівня ризику атак соціальної інженерії в банківських установах на основі аналізу поведінкових факторів і результатів сценарного опитування персоналу.

У ході дослідження встановлено, що найбільш ефективним підходом до оцінювання ризику є використання сценарних ситуацій, які моделюють типові випадки взаємодії співробітників із потенційними загрозами. Такий підхід дозволяє оцінити реакцію працівників на фішингові повідомлення, телефонні дзвінки, підроблені службові запити та інші методи психологічного впливу. При формуванні сценаріїв особлива увага приділялась доступності формулювань, відсутності складної технічної термінології та мінімізації психологічного тиску на респондентів.

Проведення сценарного опитування дало змогу отримати більш об'єктивні результати щодо поведінки працівників у потенційно небезпечних ситуаціях. Аналіз відповідей показав, що найбільшу складність для респондентів становлять ситуації, пов'язані з терміновими службовими запитами, повідомленнями від нібито керівництва та необхідністю швидкого прийняття рішень без додаткової перевірки інформації.

Для кількісного визначення рівня ризику було використано адитивну модель оцінювання на основі системи зважених балів. Кожна відповідь класифікується залежно від рівня потенційної небезпеки: 0 балів – безпечна поведінка; 1 бал – незначна необачність; 3 бали – критична вразливість. Загальний показник ризику розраховується за формулою:

$$R = \sum_{i=1}^{n} W_i$$

де R – загальний показник рівня ризику, n – кількість питань, W_i – вага обраної відповіді.

Отримані результати дозволили виокремити три основні рівні ризику. Низький рівень (0-5 балів) свідчить про достатню обізнаність працівника у сфері кібербезпеки та здатність розпізнавати потенційні загрози. Середній рівень (6-15 балів) вказує на наявність окремих прогалин у знаннях і певну схильність до психологічного впливу. Високий рівень ризику (16-45 балів) характеризує критичну вразливість співробітника, що може створювати загрозу для інформаційної безпеки банківської установи.

Результати аналізу підтверджують, що людський фактор залишається одним із найуразливіших елементів системи інформаційної безпеки. Навіть за умови використання сучасних технічних засобів захисту недостатній рівень підготовки персоналу може призвести до витоку конфіденційної інформації або несанкціонованого доступу до внутрішніх ресурсів банку. Саме тому регулярне оцінювання рівня готовності працівників до протидії атакам соціальної інженерії є важливою складовою забезпечення кібербезпеки [2].

Крім того, використання сценарного підходу дозволяє не лише визначити загальний рівень ризику, а й виявити найбільш проблемні аспекти поведінки персоналу. Це створює можливість для вдосконалення програм навчання та підвищення рівня обізнаності працівників щодо правил кібергігієни й безпечної роботи з інформацією. Проведене дослідження демонструє доцільність застосування методів оцінювання поведінкових ризиків як одного з напрямів зміцнення системи інформаційної безпеки банківських установ.

Отримані результати можуть бути використані як інформаційна основа для проведення внутрішнього аудиту безпеки, оцінювання ефективності навчальних заходів і формування рекомендацій щодо мінімізації ризиків соціальної інженерії.

Запропонований підхід дозволяє перевести поняття «людський фактор» у вимірювані показники, що підвищує ефективність управління інформаційною безпекою в банківській сфері.

Таким чином, оцінювання ризиків соціальної інженерії є важливим елементом сучасної системи захисту банківських установ. Комплексний аналіз поведінкових факторів працівників сприяє своєчасному виявленню потенційних загроз та підвищенню загального рівня стійкості організації до кіберінцидентів. Подальший розвиток методів оцінювання ризику дозволить удосконалити механізми підготовки персоналу та забезпечити більш ефективний захист інформаційних ресурсів у фінансовій сфері.

1. Бурячок В.Л. Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект. Львів: «Магнолія 2006». – 2018 – 320 с.
2. Ванацький Д. І. Соціальна інженерія. Вісник Київського інституту бізнесу та технологій, 2018. Вип. № 2 (36). – С. 26.
3. Сілін Є.С., Кадубовський О.А. Основи кібербезпеки: навчальний посібник. Дніпро, 2023. – 200 с.