Південноукраїнські наукові студії

ЗБІРНИК МАТЕРІАЛІВ

VII Всеукраїнської

науково-практичної конференції

студентів та молодих вчених

(19-21 листопада 2024 року)

Міністерство освіти і науки України
Державний заклад
«Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»
кафедра філософії, соціології та менеджменту соціокультурної діяльності
Південно-Українське відділення Соціологічної асоціації України
м. Одеса

Південноукраїнські наукові студії

ЗБІРНИК МАТЕРІАЛІВ

VII Всеукраїнської науково-практичної конференції студентів та молодих вчених

(19-21 листопада 2024 року)

УДК: 1+316 (062.552)

Рецензенти:
Володимир ЖАРКИХ, доктор філософських наук, професор, завідувач кафедри філософії, історії та політології, НУ «Одеська політехніка»;
Оксана ІВАНОВА, кандидат філософських наук, доцент, доцент кафедри мистецтвознавства та загальногуманітарних дисциплін, Міжнародний гуманітарний університет.

Рекомендовано Вченою радою Державного закладу «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського»
Протокол № 7 від 26.12.2024 р.

Південноукраїнські наукові студії: Збірник матеріалів Всеукр. наук.-практ. конф. студентів та молодих вчених (м. Одеса, 19-21 листопада 2024 року) / за ред. д. філос . н., проф. Петінової О. Б. – 213 с.

Матеріали конференції представлені в авторській редакції мовою оригіналу

Виконання зазначених вище завдань сприятиме удосконаленню наукового обґрунтування соціальних інвестицій у національній економіці шляхом формування комплексної державної політики сприяння їх розвитку. Крім того, розробка чіткої системи показників соціальних інвестицій забезпечить підвищення ефективності їх оцінки та впливу на національну економіку у розрізі фінансової та не фінансової складових.

Оцінка актуального стану соціальних інвестицій, виявлення тенденцій, проблем і можливостей розвитку соціальних інвестицій в Україні дозволить сформулювати комплекс рекомендацій щодо вдосконалення соціальних інвестицій в Україні шляхом удосконалення державної політики їх сприяння.

Аналіз ефективних іноземних практик і стратегій у сфері соціальних інвестицій дозволить отримати новий погляд на можливості їх впровадження в Україні.

Ці результати можуть суттєво вплинути на розвиток теорії і практики реалізації соціальних інвестицій, а також на формування і реалізацію державної політики в Україні щодо стимулювання їх розвитку.

Список використаних джерел:

1. Павленко І. П. Аналіз ефективності соціальних інвестицій в Україні. Економічний вісник. 2019. No 14(2). С. 45-58.
2. *Бондаренко Л. М. Соціальні інвестиції та їх роль у розвитку регіонів України. Регіональна економіка. 2021. No 8(3). С. 32-47.*
3. *Іванова М. О. Соціальні інвестиції як інструмент розвитку соціального капіталу в Україні. Соціологічні дослідження. 2023. No 22(1). С. 78-92.*
4. Левченко В. І. Соціальні інвестиції в Україні: проблеми та перспективи. Економіка і управління. 2020. No 13(2). С. 50-63.
5. Гончарук А. С. Соціальні інвестиції: глобальні тренди та українські реалії. Світова економіка. 2021. No 29(3). С. 55-72.

Ігор ГАЙДУКОВ,
здобувач третього (освітньо-наукового) рівня вищої освіти,
ОНП «Психологія»
Міжнародний гуманітарний університет, м. Одеса, Україна
Науковий керівник: Василь ЛЕФТЕРОВ, д. психол. н., професор,
Міжнародний гуманітарний університет, м. Одеса, Україна

СУЧАСНІ ТРЕНДИ У КОРПОРАТИВНОМУ ШАХРАЙСТВІ: ПСИХОЛОГІЧНІ АСПЕКТИ

Як і раніше, у 2024 році корпоративне шахрайство залишається серйозною проблемою для бізнесу в усьому світі. За даними ACFE [1] у 2024 році втрати від корпоративного шахрайства склали біля 5% всього обороту компаній.

З розвитком технологій шахраї розробляють та використовують все більш витончені схеми та постійно пристосовуються як до регуляторних змін, так і для пошуку нових вразливостей. І, як і раніше, одним з найбільш ефективних методів

шахрайських дій є, й, напевно, завжди буде атака на найслабкішу ланку у системах корпоративного захисту – людину. Саме тут шахраї вдаються до досить витончених психологічних прийомів. Нам здається цікавим не тільки описати ключові тенденції, притаманні корпоративному шахрайству у 2024 році, але й зробити це з точки зору саме психологічних аспектів. Розуміння останніх тенденцій у сфері корпоративного шахрайства може допомогти бізнесу краще підготуватися та захистити себе від фінансової та репутаційної шкоди.

1. ***Більш масштабне залучення штучного інтелекту (ШІ) у шахрайські схеми.***

Штучний інтелект, який є потужним інструментом для бізнесу, також став використовуватися у сфері корпоративного шахрайства.

Зупинимося на основних методах психологічного впливу:

1. **Маніпуляція довірою.** Шахраї, використовуючи ШІ, створюють контекст, який викликає довіру. Зокрема:

a. **Персоналізація**. Завдяки алгоритмам ШІ, шахраї можуть аналізувати дані жертв (зокрема, з соцмереж) і адаптувати таргетовані повідомлення для підвищення їх достовірності;

b. **Імітація реальних людей**. Зазвичай цей підхід використовується для створення більш складних атак, таких як технологія «глибоких підробок» (deepfake), що дозволяє видавати себе за керівників або маніпулювати фінансовими даними. Діпфейки можуть імітувати голос або відео, що полегшує обман співробітників або інвесторів. Це призвело до збільшення кількості схем компрометації ділової електронної пошти (BEC), коли шахраї видають себе за керівників високого рівня, щобсанкціонувати неправомірні банківські перекази або розкриття конфіденційних даних.

c. **Ускладнення виявлення підробки**. За допомогою ШІ шахрай може створити підроблені документи, діалоги чи відповіді на питання у реальному часі, з високою достовірністю імітуючи професіоналізм та особливості конкретної особи, що суттєво ускладнює виявлення такого типу шахрайства, особливо якщо особа, яку «підміняє» шахрай, має високий соціальний статус та певні риси характеру, які роблять «небажаним» зайвий контакт з нею. Фактично, шахрай використовує, за Р.Чалдіні, тиск авторитету [3].

2. *Ефект соціального підтвердження* [3]. ШІ здатен автоматичногенерувати фейкові відгуки, рейтинги чи коментарі, які створюютьілюзію популярності або безпеки. Люди схильні довіряти тому, що вониспринимають як підтвердження або схвалення від інших.

3. *Психологічний тиск.* Як і у випадках з персоналізацією атак, ШІ може використовувати дані про людину, щоб визначити її вразливі місця та створити контент, що має викликати:

a. *Почуття терміновості*. Наприклад, може бути сгенеровано повідомлення про блокування рахунку протягом 2 годин або відключення корпоративної пошти через годину;

b. *Страх чи тривогу*. ШІ може генерувати контент, який викликає почуття небезпеки для жертви чи її близьких;

4. *Ілюзія взаємодії с людиною*. Завдяки чат-ботам, що використовують обробку природної мови (Natural language processing (NLP)), шахраї можуть підтримувати тривалі діалоги, які здаються справжніми. Це особливо ефективно, коли людина шукає допомоги чи консультується онлайн.
5. *Когнітивна перевантаженість*. ШІ може генерувати великий обсяг інформації чи запитів, що викликає у людини складність у її обробці таприйнятті раціональних рішень. Наприклад, під час атак жертву можуть «бомбардувати» деталями, які здаються переконливими, але складними для перевірки.
6. *Зниження критичності мислення через технологічну авторитетність.* Люди часто сприймають технології, особливо такіскладні, як ШІ, як надійні. Це створює основу для зниження критичності під час взаємодії з інформацією, створеною штучним інтелектом.
7. *Автоматизація фішингових атак.* Такий тип атак за допомогою ШІ використовує технології машинного навчання (maschine learning) не тільки для аналізу корпоративного захисту та пошуку вразливостей, але й стежить за реакцією співробітників на виявлені атаки, формує патерни їх поведінки, час реакції й т.і., на основі чого генерується наступна хвиля атаки.

Тож, зараз компанії повинні розглядати наслідки застосування штучного інтелекту не лише як інструмент захисту, а й як значний вектор загроз [4]. А, виходячи з того, що дослідники з Центру майбутніх злочинів Дауеса при Університетському коледжі Лондона ще у 2020 році оцінили діпфейки як найбільшу кримінальну загрозу, пов'язану з ШІ [2], ігнорування цієї загрози може виявитися для компаній дуже коштовним.

2. ***Суттєве зростання інсайдерських загроз***

Інсайдерські загрози були постійною проблемою корпоративного шахрайства й в минулі роки, але у 2024 році вони еволюціонували. Зі збільшенням кількості працівників, які працюють віддалено, моніторинг внутрішніх загроз став більш складним завданням [1]. Внутрішніми загрозами можуть бути як працівники, які навмисно вчиняють шахрайство, так й ті, хто мимоволі допомагають шахраям, стаючи жертвами схем соціальної інженерії.

Якщо говорити про типізацію шахраїв-інсайдерів, то можна виділити наступні категорії:

- *Незадоволені працівники*. Постійно скаржаться, уникають роботи в команді, мають приховане, але стійке бажання завдати шкоди.
- *Випадкові порушники*. Зазвичай виявляють недбалість через низький рівень обізнаності або неусвідомлення ризиків.
- *Інсайдери-професіонали або «зловмисні інсайдери».* Чітко розуміють ризики своїх дій, діють обережно. Часто це колишні співробітники або ті, хто працює за наймом («треті сторони»).

Психологічними тригерами інсайдерських загроз можуть бути:

1. Стрес. Механізм впливу: Підвищений рівень стресу може знижувати здатність людини до критичного мислення та самоконтролю.

Психологічні ознаки: агресивність, самоізоляція, часті перепади настрою.

2. Низький рівень ідентифікації з організацією. Механізм впливу: Якщо співробітник не відчуває зв'язку з місією та цілями компанії, він може діяти всупереч її інтересам. Причини: відсутність підтримки з боку керівництва, нерозуміння цілей компанії, хаотичні та незрозумілі розпорядження, незрозумілі механізми оцінкироботи та оплати.
3. Когнітивне викривлення (раціоналізація). Механізм впливу: Людина може виправдовувати свої дії, вважаючи, що: «це не завдасть великої шкоди», «усі так роблять», «я заберу лише те, що мені належить».
4. Відчуття безкарності. Механізм впливу: Людина може діяти ризиковано, якщо вважає, що її дії небудуть помічені або покарані.

Таким чином, можна сформувати психологічний профіль співробітника, який може бути вразливим для корпоративного інсайдерського шахрайства. **Емоційна нестабільність:** часті зміни настрою, проблеми зі спілкуванням.
Соціальна ізоляція: обмеження контактів із колегами, уникнення командних активностей.
Схильність до ризику: недотримання правил безпеки, інтерес до потенційно небезпечних дій.
Незадоволення роботою: відчуття несправедливості, відсутністьмотивації.

5. Шахрайство в ланцюгах постачання. Шахрайство в ланцюгах постачання - ще одна зростаюча проблема у 2024 році, особливо з огляду на те, що глобалізація та складні мережі постачальниківпідвищують ризик шахрайських дій [5]. Шахраї використовують вразливі місця в ланцюгах поставок, щоб підробляти рахунки-фактури, спотворювати інформацію про товари чи послуги або займатися контрафактною діяльністю. Перехід до цифрових ланцюгів постачання та впровадження таких технологій, як блокчейн, принесли нові можливості для підвищення ефективності, але також і нові виклики у виявленні шахрайства.
Причини та тригери шахрайських дій у ланцюгах поставки подібні до інсайдерських. Проте, є декілька відмінностей:

- Групове шахрайство. Змова постачальників та/або логістичнихкомпаній.
- Тиск на досягнення результатів. Постійний тиск керівництва на швидкість, ефективність та мінімізацію витрат може сприяти шахрайству як «швидкому рішенню».

Компанії повинні переконатися, що їхні партнери по ланцюгу поставок дотримуються суворих стандартів і впроваджують ретельні процеси перевірки та моніторингу.
6. Шахрайство, пов'язане з криптовалютою та кіберзагрозами.

У міру того, як криптовалюти стають все більш популярними, шахраї знаходять нові способи їх використання [1]. Кількість шахрайств, пов'язаних з криптовалютами, різко зросла. Шахраї використовують фальшиві первинні пропозиції монет (ICO), фінансові піраміди та фішингові атаки на цифрові гаманці. Анонімність і децентралізована природа криптовалют роблять їх привабливими для шахрайських дій, оскільки їх важче відстежити порівняно з

традиційними активами.

У 2024 році бізнес все частіше стикається з ризиками, пов'язаними з атаками програм-вимагачів, які вимагають криптовалютні платежі, шахрайськими інвестиційними схемами та несанкціонованими транзакціями. Також помітно зросла кількість кібератак, спрямованих на корпоративні фінансові дані та інтелектуальну власність.

Класифікувати психологічні аспекти того, чому люди стають жертвами шахраїв можна наступним чином:

1. ***Маніпуляція емоціями:***

a. **Жадібність.** Шахраї використовують обіцянки величезного прибутку за короткий термін («тисячі відсотків доходності», «низька ризикованість» і т.і.). Причому частими є факти використання для «швидкого збагачення» саме коштів компанії.

b. **Страх пропустити можливість** (FOMO - Fear of Missing Out). Шахраї використовують те, що люди бояться пропустити «унікальну можливість» або вчасно не увійти в ринок перед «to the Moon».

c. **Стрес і паніка**. Як і у випадках з шахрайством за допомогою ШІ, шахрай викликає страх перед втратами, наприклад, інформуючи про «злам гаманця» з вимогою термінової зміни паролів.

d. **Прогресивне залучення**. Шахраї поступово збільшують вимоги до жертв: початкова невелика інвестиція з обіцянками прибутку (який може, навіть бути), після якої жертву спонукають вкладати більше.

e. **Страх втратити інвестицію**. Навіть коли жертва починає підозрювати шахрайство, вона не припиняє участь, щоб не втратити вкладені кошти, особливо, якщо це були не власні кошти.

2. ***Когнітивні упередження.***

a. *Ефект авторитету та/або соціального підтвердження* [3]. Людисхільні довіряти «експертам» або відомим особам, які рекламують криптовалюти чи проєкти, в т.ч., і за допомогою технологій deepfake, лист «від техпідтримки Microsoft» з необхідністю відреагувати тощо, лист «від банку» про необхідність термінового відвідування онлайн-банкінгу для «попередження шахрайства» (причому в останніх двох випадках копіюються всі атрибути офіційних листів компаній, їх логотипи, адреси, телефони тощо, але посилання веде на фішинговий сайт).

b. *Ілюзія контролю*. Люди часто переоцінюють свою здатність розібратися в складних фінансових механізмах та основах кібербезпеки [6].

c. *Підтверджувальне упередження* [7]. Жертви шукають інформацію, яка підтверджує їхні рішення і ігнорують не тільки попередження, але й свій попередній досвід та здоровий глузд. Людина може ігнорувати всі симптоми шахрайства, бо вірить у свою «вдачу». Особливо, коли шахрай керує цим процесом.

3. ***Недостатнє розуміння технологій.*** Багато людей не до кінця розуміють, як працюють блокчейн, токени чи криптогаманці, що робить їх вразливими до шахрайських схем. Наприклад, цим може бути обман за допомогою фальшивих

платформ для обміну криптовалют, фішинг за допомогою електронних листів та/або повідомлень у месенджерах, злам систем через «загублену» на парковці компанії флешку тощо.

Як можна побачити, кіберзагрози є не лише технічною, а й психологічною проблемою. Шахраї маніпулюють емоціями, незнанням та довірою, щоб досягти своїх цілей. Для ефективної боротьби з такими загрозами потрібен комплексний підхід, що поєднує освіту, психологічну підтримку та технологічний захист.

Щоб захиститися від цих еволюціонуючих загроз, компаніям необхідно інвестувати в передові заходи кібербезпеки, такі як багатофакторна автентифікація, шифрування та безперервний моніторинг. Навчання співробітників найкращим практикам кібербезпеки також має вирішальне значення, оскільки людські помилки залишаються основною причиною успішних кібератак.

Узагальнюючи, можна сказати, що сфера корпоративного шахрайства у 2024 році відзначається витонченістю та складністю. Оскільки шахраї продовжують розвивати свою тактику, всіляко залучаючи, крім технічних, засоби психологічного впливу, компанії повинні залишатися пильними та проактивними у своїх стратегіях захисту. Це передбачає використання технологій для виявлення шахрайства, посилення внутрішнього контролю, дотримання регуляторних вимог та розвиток культури доброчесності.

Розуміючи ці тенденції та адаптуючись до них, компанії можуть краще захистити себе від постійно зростаючої загрози корпоративного шахрайства.

Список використаних джерел:

1. Association of Certified Fraud Examiners. Occupational fraud 2024: a report to the nations. https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024- report-to-the-nations.pdf
2. Caldwell, M., Andrews, J.T.A., Tanay, T. et al. AI-enabled future crime. CrimeSci 9, 14 (2020). https://doi.org/10.1186/s40163-020-00123-8
3. Robert B. Cialdini, Influence: The Psychology of Persuasion (William Morrowe Company, 1984)
4. Deloitte. Fighting the newest trends in business fraud. Which are the most exposed processes and how can companies stay ahead of fraudsters. https://www2.deloitte.com/ro/en/pages/about-deloitte/articles/combaterea- fraudei-organizatie-care-sunt-cele-mai-expuse-procese-si-cum-pot-companiile- sa-fie-cu-un-pas-inaintea-fraudatorilor.html
5. KPMG. Supply chain fraud. https://assets.kpmg.com/content/dam/kpmg/be/pdf/Markets/supply-chain-fraud.pdf
6. Langer, E. J. (1975). The illusion of control. Journal of Personality and SocialPsychology, *32*(2), 311–328. https://doi.org/10.1037/0022-3514.32.2.311
7. Wason, Peter C. (1960), On the failure to eliminate hypotheses in a conceptualtask, Quarterly Journal of Experimental Psychology, Psychology Press, 12 (3):129—140.