управління бізнес-процесами. Ці зміни включають інтеграцію цифрових інструментів і перегляд стратегічних підходів до управління. Розвиток цифрової економіки, що ґрунтується на інноваціях, можна порівняти за значущістю з революційними етапами, такими як використання енергії пару чи електрики, проте за ефективністю цифрові технології значно їх перевершують.

Серед цифрових інструментів, які, на нашу думку, активно використовуються в аграрній сфері, слід виокремити наступні: системи управління даними (Big Data, Data Mining, хмарні обчислення, Google Analytics); інструменти взаємодії із клієнтами та постачальниками (CRM та SCM-системи, чат-боти); технології управління бізнесом (Office 365, Google Docs, дешборди для оцінки KPI); GIS- та GPS-технології для здійснення моніторингу та управління аграрними процесами та електронний документообіг, що спрощує зберігання, обробку та передачу даних.

Таким чином, цифрові технології сприяють підвищенню прозорості, оптимізації бізнес-процесів та зниженню витрат, одночасно забезпечуючи відстеження виробничих та логістичних ланцюгів, що є важливим компонентом системи продовольчої безпеки. Отже, цифрові трансформації позитивно впливають на організацію аграрного бізнесу в Україні, дозволяючи адаптувати його до умов воєнного стану та пришвидшити відновлення у післявоєнний період, сприяючи оновленню маркетингових стратегій, удосконаленню ресурсного забезпечення, спрощенню звітності та підвищенню загальної ефективності, як результат, створює основу для інноваційної системи управління в аграрній сфері.

Література:

1. Шабатура Т. С. Перспективи розвитку аграрного сектору економіки України в контексті цифрових технологій. *Приазовський економічний вісник*. 2019. Вип. 3 (14). С. 123–128

Гайдуков І. В.
аспірант спеціальності 073 «Менеджмент»
Андрощук І.О.
канд. екон. наук., доцент
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

СУЧАСНІ ТРЕНДИ У КОРПОРАТИВНОМУ ШАХРАЙСТВІ

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. Розуміння останніх тенденцій у сфері корпоративного шахрайства може допомогти бізнесу краще підготуватися та захистити себе від фінансових та репутаційних втрат.

Наведемо ключові тенденції, які притаманні корпоративному шахрайству у 2024 році:

1. Більше залучення штучного інтелекту (ШІ) у шахрайські схеми. Штучний інтелект, який є потужним інструментом для бізнесу, також став використовуватися у сфері корпоративного шахрайства. Шахраї використовують штучний інтелект 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, щоб санкціонувати неправомірні банківські перекази або розкриття конфіденційних даних. Шахрайство за допомогою ШІ також включає

автоматизацію фішингових атак і використання машинного навчання (maschine learning) для аналізу корпоративного захисту та пошуку вразливостей. Отже, зараз компанії повинні розглядати наслідки застосування штучного інтелекту не лише як інструмент захисту, а й як значний вектор загроз [2].

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. Зростає також тенденція до появи «зловмисних інсайдерів», які можуть бути незадоволеними працівниками або тими, хто прагне використати своє становище для отримання фінансової вигоди. Ці особи часто мають законний доступ до конфіденційної інформації і можуть маніпулювати нею для особистої вигоди. Щоб зменшити ці ризики, компаніям необхідно посилити свій внутрішній контроль, здійснювати регулярні аудити та сприяти розвитку етичної культури.

3. 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 постачальників підвищують ризик шахрайських дій [3].

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. Компанії повинні переконатися, що їхні партнери по ланцюгу поставок дотримуються суворих стандартів і впроваджують ретельні процеси перевірки та моніторингу.

4. 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 більш складніше відстежити порівняно з традиційними активами.

Таким чином, 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.

Саме тому, компанії мають вживати надійних заходів кібербезпеки та інформувати своїх співробітників і клієнтів про потенційні ризики, пов'язані з криптовалютами. Щоб забезпечити захист 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, слід відзначити, що сфера корпоративного шахрайства у 2024 році відзначається витонченістю та складністю. Оскільки шахраї продовжують розвивати свою тактику, компанії повинні залишатися пильними та проактивними у своїх стратегіях захисту, що 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 постійної загрози корпоративного шахрайства.

Література:

2. Association of Certified Fraud Examiners. Occupational fraud 2024: a report to the nations. URL: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2024/2024-report-to-the-nations.pdf

3. Deloitte. Fighting the newest trends in business fraud. Which are the most exposed processes and how can companies stay ahead of fraudsters. URL: 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

4. KPMG. Supply chain fraud. URL: https://assets.kpmg.com/content/dam/kpmg/be/pdf/Markets/supply-chain-fraud.pdf

Гнибіденко В.О.
здобувач гр. УФЕБ-23М
Чередніченко Н.Ю.
доктор пед. наук., професор
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

УДОСКОНАЛЕННЯ МЕХАНІЗМУ УПРАВЛІННЯ ФІНАНСОВО-ЕКОНОМІЧНОЮ БЕЗПЕКОЮ З УРАХУВАННЯМ ПОТРЕБ ЙОГО ВЛАСНИКІВ

Забезпечення економічної безпеки підприємства є складною багатофункціональною системою, яка залежить від його фінансово-економічного стану, а також від впливу внутрішніх і зовнішніх факторів. У ринкових умовах кожен суб'єкт господарювання діє автономно, застосовуючи інструменти для ідентифікації можливих загроз, які можуть негативно вплинути на його економічні інтереси та розвиток.

Економічна безпека підприємства може бути досягнута лише за умов побудови системи, яка дозволяє своєчасно виявляти, попереджувати та усувати реальні й потенційні загрози та має враховувати потреби власників підприємства, спрямовані на забезпечення його сталого функціонування.

Ефективне управління фінансово-економічною безпекою ґрунтується на чіткому розумінні ключових понять, таких як:

- економічна безпека – стан захищеності підприємства від впливу дестабілізуючих факторів;
- загроза – потенційна чи реальна небезпека для його економічних інтересів;
- ризик – ймовірність виникнення негативних наслідків;
- оцінка – визначення рівня загроз і ризиків.

Безпека є базовою умовою, яка дозволяє підприємству досягати поставлених цілей і створювати передумови для подальшого розвитку. Вважаємо, що рівень фінансово-економічної безпеки будь-якого підприємства визначається на основі:

- аналізу та діагностики діяльності, яку можливо досягти шляхом проведення оцінки технологічного рівня виробництва, конкурентоспроможності продукції та забезпеченості ресурсами, а також дослідження фінансового стану, включаючи ретроспективний аналіз і прогнозування перспектив розвитку;
- застосування різних методів оцінки. До ефективних інструментів належать експертний, рейтинговий, факторний та статистичний аналіз.

Особливу роль відіграє метод моніторингу, який дозволяє систематично спостерігати за змінами фінансово-економічного стану підприємства. Моніторинг фінансово-економічної безпеки передбачає:

- виявлення негативних тенденцій у діяльності підприємства;
- оцінку динаміки його розвитку та визначення причин загроз;
- прогнозування наслідків дії загроз;
- розробку заходів для їх усунення.