конкурентів. У цьому випадку можна створити контент, який буде нагадувати про цінність та вигоду від використання продукту чи послуги, пропонувати нові можливості, функції, опції, бонуси, знижки та інше, стимулювати повторні покупки чи передплату. Це можуть бути email-розсилки з корисною інформацією, новинами, акціями та пропозиціями для передплатників, push-повідомлення на сайті або в мобільному додатку з нагадуваннями, порадами, рекомендаціями для користувачів, програми лояльності, бонуси, подарунки, купони для заохочення постійних клієнтів [3]. Також, можна застосувати апсейл (пропозиція більш дорогого чи додаткового продукту) чи кроссейл (пропозиція супутнього продукту) з метою збільшення середнього чека і повторних продажів.

Правильне формування інформаційного контенту сприяє залученню цільової аудиторії, стимулює потенційного клієнта до дій та супроводжуватиме його до моменту укладання угоди. Висока якість контенту формує довіру та лояльність до бренду компанії, демонструє її експертність та авторитетність та у кінцевому підсумку забезпечує стабільне зростання клієнтської бази та обсягів продаж.

Інформаційні джерела

1. Витвицька О. М., Суворова С. Г., Корюгін А. В. Вплив цифрового маркетингу на розвиток підприємництва в умовах війни. Економіка та суспільство. 2022. Вип. 40. URL: https://economyandsociety.in.ua/index.php/journal/article/download/1518/1460

2. Кривко О. Якими будуть користувачі у 2024 році. URL: https://skvot.io/uk/blog/yakimi-budut-koristuvachi-u-2024

3. Кушнір Д. Маркетинг у 2024 році: погляд у майбутнє і головні тренди. URL: https://marketer.ua/ua/marketing-in-2024-a-look-into-the-future-and-major-trends/

УДК 657.6:640.342

Н.С. Ковалевська, канд. екон. наук, проф. *(ДБТУ, Харків)*

АУДИТОРСЬКА ОЦІНКА КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНОГО РИЗИКУ В ГОТЕЛЬНОМУ БІЗНЕСІ

На кожному з етапів інформаційного сервісу підприємств готельного бізнесу виникають внутрішньогосподарські ризики. Згідно з міжнародними стандартами аудиту аудиторський ризик складається з внутрішньогосподарського (властивого) ризику, ризику контролю та ризику не виявлення [1, с. 367]. Незважаючи на те, що системою внутрішнього аудиту здійснюється не вибіркова, а суцільна перевірка

діяльності готельного підприємства, йому притаманні такі ж групи ризиків, але їх оцінка на стадії планування має свої особливості. Так, на початковій стадії планування важливо чітко визначити мету аудиту і створити стратегію оцінки ризиків, що допоможе сконцентруватися на найбільш суттєвих аспектах безпеки. З метою ідентифікації потенційних загроз внутрішні аудитори проводять аналіз слабких місць в системі безпеки. Враховуються всі можливі сценарії загроз, включаючи кібератаки, витоки даних, недостатній контроль доступу тощо. Проводиться оцінка ефективності внутрішнього контролю щодо запобігання ризикам, що включає перевірку систем контролю доступу, моніторинг та системи реагування на події [2, с. 214].

Оцінка ризиків допомагає визначити обсяг і глибину аудиту, дозволяє сконцентрувати зусилля на найбільш критичних для безпеки аспектах. На основі виявлених ризиків створюється план дій для подальшого проведення аудиту, включаючи необхідні заходи для мінімізації виявлених ризиків. Інформаційні ризики в готельній галузі можуть виникати з різних джерел та мати різні прояви:

1) кібербезпека – ризик охоплює загрози кібератак, викрадення даних, віруси, атаки на мережу та інші кіберзлочини, що можуть призвести до витоку конфіденційної інформації;

2) зберігання та обробка даних – недостатня безпека в обробці та зберіганні особистої інформації гостей може призвести до порушень приватності та витоку конфіденційної інформації;

3) фінансові ризики – включають можливість фінансових шахрайств, втрати фінансової інформації, крадіжки грошей тощо;

4) недостатній контроль доступу – якщо інформація доступна для недостатньої кількості осіб або якщо немає належних контрольних механізмів, це може призвести до порушення безпеки;

5) соціальний інжиніринг – атаки, спрямовані на спокусу персоналу готелю на надання доступу до систем або інформації;

6) технічні проблеми - несправності апаратного забезпечення, програмного забезпечення або неправильна настройка систем;

7) недостатня освіта та навички персоналу – якщо персонал не має достатніх знань про кібербезпеку та правила безпеки, це може призвести до вразливостей у системах [3, с. 130].

Для готелів важливо ретельно оцінювати та управляти цими ризиками, використовуючи технології та політику безпеки, щоб захистити конфіденційні дані гостей та забезпечити безпечну роботу систем управління готелем. Аудиторська оцінка інформаційного ризику підприємств готельного бізнесу полягає в перевірці та оцінці рівня загроз, які можуть виникнути внаслідок обробки, зберігання та

передачі інформації в готельному бізнесі. Основні аспекти такої оцінки включають: збір і аналіз даних; оцінку потенційних загроз; перевірку внутрішнього контролю; оцінку рівня вразливості; рекомендації щодо поліпшення безпеки. В процесі проведення перевірки внутрішньому аудитору необхідно перевірити правильність визначення собівартості послуг готельного підприємства за сегментами, що дозволить оптимізувати цінову політику. Операційна документація показує сутність і обсяг надання готельних послуг, що є основою для визначення виручки від реалізації та собівартості готельних послуг та відображення в обліку отриманих авансів. Для кожного виду готельних послуг враховується тип операції (готівка, ціна, виплати) та її грошова вартість [4, с. 164].

Для цілей внутрішнього аудиту облікова система має забезпечувати додаткову, незалежну документацію для перевірки кожної операції. У ручній або напівавтоматичній операції підтверджуючі документи, створені будь-якими методами, служать джерелами перехресних посилань. А аудитор, отримавши інформацію про зайнятість готельних номерів і маючи дані за їх розцінками, порівнює все зі звітом служби прийому та розміщення.

Для аудиторської оцінки кібербезпеки в готельному бізнесі доцільно використовувати різні методи, інструменти та підходи, а саме: проведення повного аудиту інформаційної безпеки для виявлення потенційних загроз та слабких місць у системах та мережах готелю; пентестинг (тестування на проникнення), тобто симуляція кібератак для виявлення вразливостей в системах та програмному забезпеченні готелю; моніторинг безпеки (використання спеціалізованих програм для постійного моніторингу мережі та виявлення незвичайних або підозрілих активностей); шифрування даних (застосування шифрування для захисту конфіденційної інформації та даних клієнтів готелю); фізична безпека (заходи безпеки для фізичного забезпечення серверних кімнат та інших інфраструктурних об'єктів, де зберігається чутлива інформація); проведення навчання та тренінгів для персоналу щодо кібербезпеки та процедур безпеки; забезпечення оновлення програмного забезпечення та застосунків для запобігання вразливостей та атак [5, с. 490]. Дані методи та підходи є лише деякими засобами забезпечення кібербезпеки службами внутрішнього аудиту в готельній галузі та використовуються для мінімізації ризиків та захисту конфіденційної інформації. Наступною складовою ризику внутрішнього аудиту на готельних підприємствах є інвестиційний ризик, оцінка якого набуває актуальності в умовах збільшення частки акціонерних підприємств

готельного бізнесу.

Таким чином, в умовах постійних змін економічного простору розширюється й сфера впливу ризиків, виникнення яких в подальшому може призвести до негативних результатів діяльності готелів. Тому оцінка ризиків має здійснюватися в системі внутрішнього аудиту постійно, з метою їх зниження до прийнятного рівня. Саме аудит інформаційного ризику в готельному бізнесі допомагає забезпечити безпеку обробки та збереження даних, захист конфіденційної інформації клієнтів, надійність систем управління готелем.

Інформаційні джерела

1. Міжнародні стандарти контролю якості, аудиту, огляду, іншого надання впевненості та супутніх послуг. Ч. І. К.: Міжнародна федерація бухгалтерів, Аудиторська палата України. 2018. 1442 с.

2. Nesterenko I. V., Kovalevska N. S., Sokolova E. B. Modeling Accounting Policies for the Hospitality Industry in the Context of Globalization. *Бізнес Інформ*. 2020. № 6. P. 212-218. URL: https://repo.btu.kharkov.ua//handle/123456789/10058

3. Фабіянська В.Ю. Комп'ютерний аудит в Україні в контексті вимог європейського законодавства. *Облік і фінанси*. 2019. № 3 (85). С. 129–137.

4. Ковалевська Н. С., Нестеренко І. В., Соколова Є. Б., Карбівнича Т. В. Цифровий компонент сучасного аудиту діяльності суб'єктів підприємницької діяльності. *Бізнес Інформ*. 2021. № 4. С. 161-168. URL: https://repo.btu.kharkov.ua//handle/123456789/10062

5. Михалик М.В., Чубай В.М. Методи оцінювання рівня аудиторського ризику: особливості, переваги та недоліки. *Молодий вчений*. 2019. № 1 (65). С. 486-491.

6. Kashchena N., Kovalevska N., Nesterenko I. Organizational and methodological aspects of audit of integrated reporting of enterprise. Zeszyty naukowe wyższej szkoły technicznej w katowicach. Wyższej Szkoły Technicznej w Katowicach. 2021. S. 153–164. URL : http://www.wydawnictwo.wst.pl/uploads/files/b0476ba555ccaead5a41dfab07ee2f39.pdf

УДК 334.012.63/.64 : 355(477)

М.Я. Кобеля-Звір, канд. екон. наук (PhD) *(ЛТЕУ, Львів)*

ГРАНТИ ЄВРОПЕЙСЬКОГО БАНКУ РЕКОНСТРУКЦІЇ ТА РОЗВИТКУ НА КОНСАЛТИНГОВІ ПОСЛУГИ ДЛЯ МІКРО-, МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ УКРАЇНИ

Україна є членом ЄБРР із серпня 1992 р. Це зазначено у відповідному Указі Президента України від 14.07.1992 № 379/92 [1], згідно з яким наша країна приєдналася до Угоди про заснування