

Секція 3

ІННОВІНГ ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ТУРИСТИЧНІЙ ДІЯЛЬНОСТІ

АХМЕДОВА Олена, д.держ.упр., доцент

Київський національний університет технологій та дизайну, м.Київ

ЄРМАКОВ Іван, аспірант кафедри підприємництва, торгівлі і туристичного бізнесу

Харківський національний економічний університет ім. С. Кузнеця, м.Харків

КІБЕРБЕЗПЕКА У СФЕРІ ТУРИЗМУ В ЕПОХУ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Постановка проблеми. Безпека та захист є ключовими передумовами для розвитку подорожей і туризму. Глобальні зміни, що відбуваються в останні десятиліття, мають масштабний характер. Негативний вплив цих подій виявив вразливість туристичного сектора як на глобальному, так і на регіональному рівнях. Зважаючи на зазначені виклики, а також на активний перехід багатьох процесів у цифрове середовище, виникає необхідність у глибокому вивченні взаємозв'язку між питаннями безпеки та туризму. Особливу увагу слід приділити кібербезпеці туристичних послуг у контексті сучасних загроз, враховуючи актуальні виклики й особливості цифрової епохи.

Виклад основного матеріалу. Цифрова трансформація галузі подорожей і туризму, яка охоплює онлайн-транзакції, аналітику клієнтських даних, інтеграцію з хмарними сервісами та цифрові платіжні технології, супроводжується усвідомленням зростаючих ризиків. Зі збільшенням цифрового сліду організації стають все більш вразливими до атак у кіберпросторі.

Кібератаки можуть мати значний вплив на довіру клієнтів і репутацію бренду, спричиняючи серйозні фінансові, юридичні та регуляторні наслідки. За даними Kaspersky Lab [1], витрати на відновлення компанії після порушення кібербезпеки перевищують \$500 000 США. Ця сума охоплює прямі збитки, такі як витрати на відновлення IT-інфраструктури, компенсацію втрат бізнесу через простої, а також витрати на юридичні послуги і зв'язки з громадськістю. Додаткові непрямі витрати, пов'язані з наймом і навчанням персоналу, модернізацією інфраструктури тощо, оцінюються в середньому в \$70 000 [1].

Однією з найбільш вразливих до кіберзлочинності галузей є сфера подорожей і туризму, де готельно-ресторанні комплекси посідають третє місце за кількістю випадків компрометації після підприємств роздрібної торгівлі та фінансових установ. Великі обсяги онлайн-бронювань подорожей та прогнозоване подальше їх зростання щорічно на 6,2% до \$552 млн. на рік [2], завжди були точкою тяжіння для кіберзлочинців. Цей сектор ще дуже привабливий тим, що дані клієнтів зберігаються на безлічі комп'ютерів, серверів і мереж готелів, авіакомпаній, компаній з бронювання та прокату автомобілів, навіть ресторанів і барів. Очікується, що до 2029 року онлайн-продажі становитимуть 75% від загального доходу на ринку подорожей і туризму, що тільки збільшить кількість кіберзагроз.

На рисунку представлено співвідношення офлайн і онлайн бронювань та їх прогнозовані дані [2].

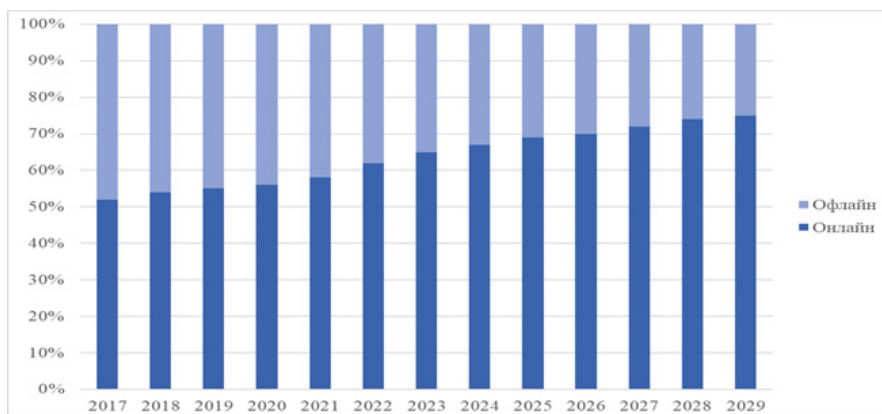


Рис. Канали продажів у сфері подорожей і туризму (станом на липень 2024)

Найбільшим ринком у галузі подорожей і туризму є ринок готелів, який, за прогнозами, досягне обсягу 426,50 млрд доларів США у 2024 році. Очікується, що кількість користувачів на ринку готелів збільшиться до 1 814,00 млн користувачів до 2029 року. У 2024 році рівень проникнення користувачів становив 25,6%, а до 2029 року, за прогнозами, він досягне 32,8%. Середній дохід на одного користувача сягатиме 0,46 тис. доларів США [2].

Висновки. З огляду на значну кількість збоїв та порушень кібербезпеки, забезпечення захисту даних і конфіденційності поступово стає однією з ключових конкурентних переваг у сфері туризму. Управління ідентифікацією та доступом (IAM) все більше розглядатиметься з точки зору забезпечення зручності для клієнтів. У результаті туристичні агенції та оператори будуть орієнтуватися на впровадження рішень, які забезпечують гнучкість, зокрема використання моделей надання послуг, таких як IDaaS і PAMaaS. Ці моделі пропонують передові рішення, включаючи безпарольну автентифікацію, єдиний вхід (SSO) та багатофакторну біометричну автентифікацію. Зростаюча кількість організацій у секторі туризму переводить свою ІТ-інфраструктуру та центри обробки даних у хмарні середовища, тобто «мультихмарний підхід» стає все більш популярним для вирішення таких завдань, як розподілене бронювання, управління доходами, управління каналами дистрибуції, робота кол-центрів та управління контентом. Такий підхід забезпечує гнучкість, відмовостійкість і значні економічні переваги.

Водночас використання мультихмарних рішень ускладнює безпечне управління системами та інформаційними активами. Це підвищує ризик роз'єднаної видимості та непослідовного впровадження засобів кібербезпеки. Двома основними викликами для організацій у галузі туризму будуть, по-перше, забезпечення відповідності вимогам стандарту PCI DSS при передачі персональних даних через різні хмарні середовища, і, по-друге, розробка інтегрованої стратегії запобігання загрозам, яка включатиме автоматизоване виявлення загроз та реагування на них.

Література

1. Kaspersky Lab. Incident response analyst report (2023). URL: <https://securelist.com/kaspersky-incident-response-report-2023/112504/>.
2. Statista. (2024). URL: <https://www.statista.com/>