2. Making Tourism More Sustainable. A Guide for Policy Makers, UNEP and UNWTO. URL: http://sdt.unwto.org/content/about-us-5.

3. Цілі сталого розвитку. Національна доповідь URL: https://www.kmu.gov.ua/storage/app/sites/1/natsionalna-dopovid-csr-Ukrainy.pdf

УДК 338.48:004.7

***Шевченко О.О.**, к.е.н, доц.*
***Дуброва Д.М.**, бакалавр*
Київський національний університет технологій та дизайну

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ПРИ ОНЛАЙН-ПРОДАЖАХ ГОТЕЛЬНИХ ПОСЛУГ У МЕРЕЖІ RADISSON BLUE

У сучасному світі, де онлайн технології стали неодмінною частиною нашого життя, безпека та конфіденційність стають основоположними принципами для успішного функціонування будь-якої онлайн-платформи. Особливо важливою є безпека при онлайн-продажах готельних послуг, коли клієнти передають свої персональні дані та здійснюють фінансові транзакції.

Мережа готелів Radisson Blue, яка володіє престижем та надійністю, розуміє важливість забезпечення безпеки та конфіденційності своїх клієнтів. Проте, відомо, що це завдання стикається з численними викликами. Один з найбільших викликів полягає у захисті особистої інформації клієнтів від несанкціонованого доступу та зловживання [1].

Перш за все, необхідно використовувати сучасні технології шифрування та захисту даних для забезпечення безпеки передачі та зберігання інформації. Це включає використання протоколів HTTPS, які забезпечують захищене з'єднання, та шифрування даних, що передаються між клієнтом і сервером.

Крім того, ефективний механізм контролю доступу до інформації та обмеження прав доступу співробітників гарантує захист конфіденційної інформації. Важливо, щоб лише авторизовані співробітники мали доступ до

цієї інформації, і щоб вони мали тільки необхідні повноваження для виконання своїх обов'язків.

Окрім технологічних заходів, важлива роль у забезпеченні безпеки та конфіденційності належить навчанню персоналу. Налагодження культури кібербезпеки серед працівників та навчання їх професійним навичкам уникнення шахрайства та фішингових атак може суттєво знизити ризик інцидентів.

Додатково, варто впроваджувати системи моніторингу та виявлення вторгнень для вчасного виявлення та реагування на потенційні загрози безпеці інформації. Це дозволить швидко виявляти незвичайну активність та запобігати можливим порушенням безпеки.

Співпраця з провідними кібербезпековими експертами та використання їхніх рекомендацій є ще однією стратегією для забезпечення безпеки і конфіденційності. Це допоможе мережі Radisson Blue бути на передовій технологічного розвитку та гарантувати найвищий рівень безпеки для своїх клієнтів.

Важливим аспектом є також аудит безпеки системи та періодичні тестування на проникнення. Це дозволяє виявляти слабкі місця в системі та вчасно вживати заходів для їх усунення.

Нарешті, безпека та конфіденційність повинні бути забезпечені не тільки на етапі онлайн-продажу, але і під час зберігання та обробки персональних даних після транзакції. Застосування надійних систем зберігання даних та встановлення строгих правил доступу є важливими складовими безпеки.

Загалом, забезпечення безпеки та конфіденційності при онлайн-продажах готельних послуг у мережі Radisson Blue є багатоаспектним завданням, яке потребує поєднання технологічних, організаційних та людських ресурсів. Тільки шляхом постійного вдосконалення і впровадження

найкращих практик можна забезпечити високий рівень безпеки та конфіденційності для клієнтів мережі Radisson Blue.

Після проведення аналізу стану забезпечення безпеки та конфіденційності при онлайн-продажах готельних послуг у мережі Radisson Blu [2, 3] можна виділити наступні ключові напрямки, які потребують постійної уваги:

- використання сучасних технологій шифрування та захисту даних є необхідною стратегією для забезпечення безпеки та конфіденційності;
- налагодження ефективного механізму контролю доступу до інформації та обмеження прав доступу співробітників до персональних баз даних;
- навчання персоналу щодо кібербезпеки та обізнаності з методами запобігання шахрайству та фішинговим атакам;
- впровадження системи моніторингу та виявлення вторгнень допомагає вчасно виявляти та реагувати на потенційні загрози безпеці інформації;
- співпраця з провідними кібербезпековими експертами та використання їхніх рекомендацій допомагає покращити стратегію безпеки мережі;
- періодичний аудит систем безпеки та тестування щодо попередження стороннього проникнення та виявлення слабких місць;
- забезпечення безпеки не тільки на етапі онлайн-продажу, але і під час зберігання та обробки персональних даних після транзакції;
- врахування регуляторних вимог та стандартів щодо захисту конфіденційності і персональних даних гарантує відповідність вимогам безпеки тощо.

Водночас, варто відзначити, що вирішення проблем безпеки та конфеденційності, які виникають унаслідок прогалин у різних частинах кіберпростору значно спрощується при впровадженні міжнародних стандартів

(наприклад із серії ISO/IEC 27032:2016), які містять технічні рекомендації для подолання таких ризиків [6].

Література

1. Готельна група Radisson. Конфіденційність і безпека. Офіційний сайт. URL: https://www.radissonhotels.com/uk-ua/privacy

2. Готельна група Radisson. Онлайн-безпека. Офіційний сайт. URL: https://www.radissonhotels.com/uk-ua/online-security

3. Hospitality Technology. Кібербезпека в готелі: захист даних та гостей. Офіційний сайт. URL: https://hospitalitytech.com/hotel-cybersecurity-protecting-data-and-guests

4. Hospitality Net. Конфіденційність та безпека даних: виклики та рішення для готелів. URL: https://www.hospitalitynet.org/opinion/4086563.html

5. Hotel Tech Report. Кібербезпека в готелі: як захистити гостей і свій бізнес. URL: https://hoteltechreport.com/news/hotel-cybersecurity

6. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT)