https://doi.org/10.31891/2307-5740-2024-328-42
УДК: 338.48

РУДЕНКО Микола
Черкаський національний університет ім. Богдана Хмельницького
https://orcid.org/0000-0002-1966-7695
mykola_rudenko@ukr.net
КОЧУМА Інна
Черкаський національний університет ім. Богдана Хмельницького
https://orcid.org/0000-0002-4416-3333
innkoc@gmail.com
КРАВЧЕНКО Олена
Черкаський національний університет ім. Богдана Хмельницького
https://orcid.org/0000-0002-8776-4462
olena_kravchenko17@ukr.net
ТРЕТЯК Наталя
ПВНЗ «Європейський університет»
https://orcid.org/0000-0002-9457-2645
natali_m2008@ukr.net

ІНФОРМАЦІЙНА БЕЗПЕКА В SMART-ТУРИЗМІ: УПРАВЛІННЯ РИЗИКАМИ, МАРКЕТИНГОВІ СТРАТЕГІЇ, ПЕРСПЕКТИВИ

У статті досліджено інформаційну безпеку в smart-туризмі та запропоновано інструменти управління ризиками, маркетингові стратегії, перспективи. Окреслено основні елементи Smart-туризму. Виділено компонентний склад Smart-туризму, який базується на основі накопичення, обміну та обробки великих масивів інформації з застосуванням інформаційно-комунікаційних технологій. Виявлено, що першочерговим завданням на шляху забезпечення інформаційної безпеки в Smart-туризмі є виявлення причин несанкціонованого доступу до інформації, оцінка загроз для інформаційної безпеки його суб'єктів та створення потужних систем її захисту. Побудовано комплексну систему інформаційної безпеки туристичного підприємства з деталізацією його елементного складу та зазначено, що захист має здійснюватися на усіх етапах життєвого циклу інформації, з урахуванням новітніх тенденцій і явищ в сфері розвитку цифрових технологій.

Ключові слова: інформаційна безпека, smart-туризм, діджиталізація, кібербезпека, туристичні підприємства, smart-маркетинг, цифрові технології, управління ризиками, маркетингові стратегії.

RUDENKO Mykola, KOCHUMA Inna, KRAVCHENKO Olena
Bohdan Khmelnytsky National University of Cherkasy
TRETYAK Natalia
PHEI «European University»

INFORMATION SECURITY IN SMART TOURISM: RISK MANAGEMENT, MARKETING STRATEGIES, PERSPECTIVES

The article examines information security in smart tourism and offers risk management tools, marketing strategies, and prospects.

The main elements of Smart-tourism are outlined, among which Smart-infrastructure (the use of the Internet of Things (IoT), artificial intelligence, sensors, cameras and other technologies to improve the management of tourist attractions and services), Smart-mobility (development and distribution of mobile applications) , which allow tourists to quickly find information about transport, routes, places of interest, etc.), Smart-communication (use of messengers, chatbots and other means of communication to provide information and support to tourists), Smart-marketing (use of digital platforms for advertising tourist services and attraction of new customers, personalized services, interactive technologies), Smart ecology (development of environmental protection technologies and support of environmental initiatives in the field of tourism).

The component composition of Smart-tourism, which is based on the accumulation, exchange and processing of large arrays of information with the use of information and communication technologies, is highlighted. "Smart direction" involves the integration of information and communication technologies into the physical tourist infrastructure. "Smart business" means the digitalization of core processes and the creation of a complex ecosystem. The smart experience component is about improving and enriching the experience through personalization, real-time monitoring.

It was revealed that the primary task in the way of ensuring information security in Smart-tourism is to identify the causes of unauthorized access to information, assess threats to the information security of its subjects and create powerful systems for its protection. A comprehensive system of information security of a tourist enterprise was built, detailing its elemental composition, and it was stated that protection should be carried out at all stages of the life cycle of information, taking into account the latest trends and phenomena in the field of digital technology development.

Keywords: information security, smart tourism, digitalization, cyber security, tourist enterprises, smart marketing, digital technologies, risk management, marketing strategies.

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Військова агресія російської федерації, а особливо її повномасштабне вторгнення після 24 лютого 2022 року радикально загострили ряд безпекових проблем в усіх сферах життя українського суспільства, в

усіх галузях, зокрема в туристичній, яка зіткнулись зі знищенням та руйнуванням матеріальних ресурсів, дефіцитом висококваліфікованого персоналу, стрімким скороченням туристичних потоків та зміною їх напрямків. Додались проблеми, пов'язані зі знищенням ворогом енергетичної та комунальної інфраструктури, з дефіцитом електроенергії, води, тепла, інших засобів життєзабезпечення, фінансовими проблемами.

Але не менш актуальними для туристичної сфери стали воєнні небезпеки в результаті збройних та терористичних атак агресора на об'єкти її інфраструктури, готелі, туристські бази, ресторани тощо. Проведені дослідження дозволяють припустити, що в їх основі міг бути витік інформації через недостатню її захищеність. Не меншу небезпеку створюють кібератаки, які можуть здійснюватися не лише шахраями, але й ініціюватись ворогом. Її об'єктом можуть стати масиви інформації, які використовуються в рамках концепції в Smart-туризму, що потребує особливої уваги до питань її захисту та безпеки. Це, в свою чергу зумовлює потребу в ретельній роботі над дослідженням проблем інформаційної безпеки в умовах російсько-української війни та післявоєнної відбудови та розробкою напрямів до її мінімізації, управління ризиками, пошуку маркетингових стратегій розвитку та окреслення майбутніх перспектив функціонування галузі.

Інформаційна безпека в сучасному Smart-туризмі стає все більш актуальною, особливо з розвитком цифрових технологій. Важливим в контексті інформаційної безпеки є ризики виникнення кібератак та крадіжок особистих даних. Подорожуючи в інші країни, чи регіони в межах нашої держави людина використовує велику кількість особистих даних, які можуть бути підвладні кіберзлочинцям. Тому важливо приділяти увагу захисту особистих даних, підтримувати їх конфіденційність з використання можливостей сучасних технологій захисту інформації (використання надійних віртуальних приватних мереж (VPN), регулярне оновлення програмного забезпечення на пристроях, уникання підключення до ненадійних Wi-Fi мереж тощо).

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Слід зазначити, що проблеми інформаційної безпеки, в діяльності суб'єктів господарювання є об'єктом активних наукових досліджень вітчизняної та світової наукової спільноти. Інформаційна безпека виходить на передній план у сучасному світі, де кіберзлочинність та кібератаки становлять серйозні загрози для бізнесу та інших сфер діяльності. Вчені та практики по всьому світу працюють над розробкою нових технологій та стратегій для захисту інформації та даних від несанкціонованого доступу.

Питанням інформаційної безпеки присвячено роботи таких вітчизняних науковців, як Горник В.Г., Ляшенко О.М., Маркіна І.А, Нашинець-Наумова А. Ю., Нехай В.А, Рач В.А., Ткачук Т.Ю., Шевчук М.О. та багатьох інших. Водночас робота над визначенням сутності та значення Smart-туризму як перспективного напряму розвитку туристичної галузі в Україні. Зокрема цим питанням присвячені роботи Воронкова В.Г., Воскресенської О.Є., Дичковського С.І., Зінов`євої І.С., Радченко О.М., Ящишиної І.В. Однак проблеми синергічного поєднання необхідності захисту інформації, що накопичується, обмінюється, обробляється в системі Smart-туризму в умовах воєнного стану та післявоєнної відбудови поки що не знайшли достатнього відображення у вітчизняній науковій літературі, що потребує поглиблення досліджень в окресленому напрямку та пошуку інструментів управління ризиками, маркетингових стратегій, а також визначення майбутніх перспектив розвитку.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Мета статті: провести аналіз впливу інформаційної безпеки на розвиток Smart-туризму в Україні з метою визначення основних ризиків та небезпек для суб'єктів туристичного бізнесу шляхом виділення ключових елементів Smart-туризму, розробки рекомендацій щодо інструментів забезпечення інформаційної безпеки та окреслення маркетингових стратегій, зумовлених розвитком туристичної галузі в умовах воєнного стану та післявоєнної відбудови.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Поняття «розумного туризму» з'явилося в результаті Директиви Європейського Союзу про розумний туризм. Він передбачає надання туристських послуг на основі використання мобільних додатків, штучного інтелекту, Big Data, віртуальної реальності та інші цифрових рішень, що дозволяє досягти більшої зручності, персоналізації та підвищення якості туристського обслуговування, розширення взаємодії туристів з природним та культурним середовищем місць відвідування.

Слід зазначити, що існують різні підходи до розуміння сутності та змісту Smart-туризму. Так, Gretzel1 U., Sigala M., Xiang Z., Koo C. [1, с. 48] визначають його як туризм, що підтримується комплексними зусиллями зі збору, агрегації, використання даних, отриманих з фізичних структур, соціальних зав'язків, урядових джерел, у поєднанні з використанням передових технологій для перетворення цих даних у локальний досвід та цінні пропозиції з чітким фокусом на ефективність, стійкість та збагачення досвіду. При цьому, вони відрізняють Smart-туризм та електронний туризм.

Воронкова В. Г. та Череп А. В. розглядають Smart-туризм як різновид Data Science туризму, який «дозволяє мандрівникам розвивати творчі здібності, використовувати інформаційні креативні технології для

створення нових високотехнологічних туристичних продуктів та послуг, націлених на самоактуалізацію та пошук чогось нового у процесі використання туристичної діяльності» [2, с. 168].

Воскресенська О. Є. та Зіновєва І. С. розкривають його зміст за допомогою таких його складових як: «Smart-туристська компанія (фірма) – організація, що працює в сфері туризму, в якій використання в бізнесі смарт-елементів призводить до принципово нової якості процесів, що підвищує ефективність комерційної діяльності та конкурентоспроможність фірми; Smart-турист – споживач туристської послуги, який постійно використовує Smart-елементи для досягнення нової якості процесів в туризмі, з метою найбільш повного задоволення своїх туристських потреб; Smart-процес (в туризмі) – процес надання туристичної послуги, який дає можливість ефективного задоволення потреб Smart-туриста» [3, с. 228].

Smart-туризм – це концепція розвитку туризму, яка базується на використанні сучасних технологій для покращення якості туристичних послуг і забезпечення більш комфортного досвіду для відвідувачів. На основі аналізу літературних джерел [1-3] виділимо основні елементи Smart-туризму (рис. 1).

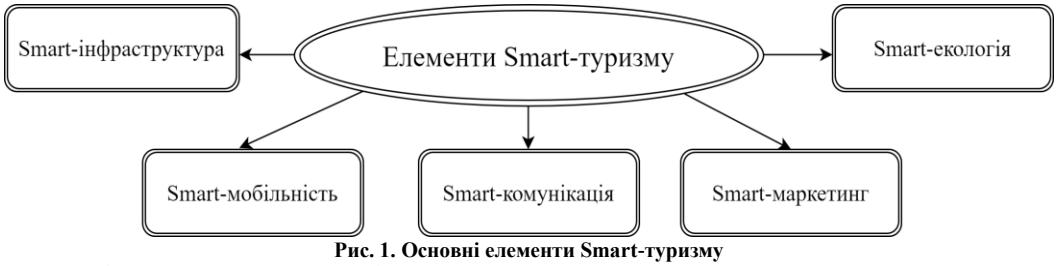

Рис. 1. Основні елементи Smart-туризму

Джерело: сформовано авторами на основі [1-3]

Деталізуємо основні елементи Smart-туризму наведені на рисунку 1:

– Smart-інфраструктура передбачає використання Інтернету речей (IoT), штучного інтелекту, сенсорів, камер та інших технологій для покращення управління туристичними пам'ятками та послугами;

– Smart-мобільність відбувається за рахунок розвитку та поширення мобільних додатків, які дозволяють туристам швидко знаходити інформацію про транспорт, маршрути, визначні місця тощо;

– Smart-комунікація потребує використання месенджерів, чат-ботів та інших засобів зв'язку для надання інформації та підтримки туристів;

– Smart-маркетинг передбачає використання цифрових платформ для реклами туристичних послуг та залучення нових клієнтів, персоналізовані послуги, інтерактивні технології;

– Smart-екологія стимулює розвиток технологій збереження навколишнього середовища та підтримки екологічних ініціатив в галузі туризму.

Наведені елементи допомагають покращити ефективність та доступність туристичних послуг, а також зробити туристичний досвід більш інтерактивним та захоплюючим для потенційних клієнтів та споживачів туристичних послуг.

В європейському співтоваристві поняття Smart-туризм почало застосовуватись в контексті розвитку т. з. Smart-міст. Зокрема з 2018 року проводиться конкурс на звання європейської столиці з Smart-туризму. В 2023 році з-поміж 29-ти міст з 13-ти європейських країн переможцями стали м. Пафос (Кіпр), Севілья (Іспанія). [4]. Міста-учасники конкурсу, оцінювались за основними критеріями: доступність, сталість та цифровізація. З огляду на такий підхід Smart-туризм визначається як напрямок, що полегшує доступ до туристичних і гостинних продуктів, послуг, просторів і досвіду за допомогою інноваційних рішень на основі інформаційно-комунікаційних технологій, що роблять туризм стійким і доступним, та дозволяє повністю використовувати культурну спадщину та творчість [5].

Розвиток Smart-туризму став загально-європейським та світовим трендом і Україна є однією з країн, що впроваджує його кращі практики. Основними компонентами Smart-туризму є: розумні напрямки, розумний бізнес і розумний досвід (рис. 2).

Компонентний склад Smart-туризму (рис. 2) базується на основі накопичення, обміну та обробки великих масивів інформації з застосуванням інформаційно-комунікаційних технологій. «Розумний напрямок» передбачає інтеграцію інформаційно-комунікаційних технологій у фізичну туристську інфраструктуру для забезпечення мобільності, розподілу ресурсів і забезпечення стабільної якості життя для жителів територій і мандрівників. «Розумний бізнес» означає цифровізацію основних процесів і створення складної екосистеми з тісною державно-приватним партнерством задля обміну ресурсами та спільного створення туристичного досвіду. Компонент «розумний досвід» стосується покращення та збагачення досвіду за допомогою персоналізації, моніторингу в реальному часі та контекстно-залежних послуг [5].

Деякі дослідники до елементів Smart-туризму відносять також нейронний маркетинг. Мається на увазі технологія, спрямована на стимулювання споживчого попиту, на основі врахування закономірностей роботи людської підсвідомості, яка впливає на вчинки людини [7]. Smart-туризм є важливим чинником розвитку міжнародного туризму та включення української туристичної галузі до світової туристичної

системи, зростання вхідних та вихідних туристських потоків, інвестицій, соціально-економічного розвитку територій.

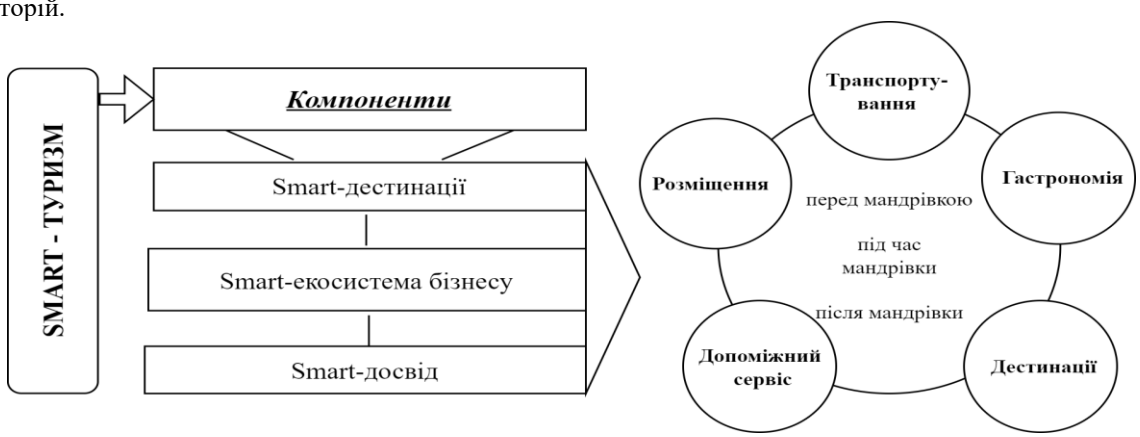

Рис. 2. Компонентний склад Smart-туризму

Джерело: сформовано авторами на основі [6]

Базисом Smart-туризму, як зазначалось вище, є використання інформаційно-комунікаційних технологій, що застосовується для збору, обміну та обробки великих масивів інформації у галузі подорожей та гостинності. Завдяки їй, користуючись електронними платформами, додатками, сайтами, мандрівник може обрати найоптимальніший для себе маршрут, мінімізувати витрати часу і грошей, орієнтуватись у просторі і на новому місці. З іншого боку, завдяки їй надавачі туристичних послуг мають змогу будувати ефективні маркетингові стратегії, створювати для мандрівників максимально персоналізовані пропозиції, оптимізувати використання туристичних ресурсів, інвестувати в туристичну інфраструктуру на перспективу, тим самим підвищуючи свою конкурентоспроможність.

Однак концентрація великих масивів інформації, часто конфіденційної, породжує небезпеку несанкціонованого доступу до неї та використання у злочинних цілях. Як зазначають Дячек О.Ю., Рябченко К. М. «Цифрові дані … не підпадають під жодні правила, які застосовуються до звичайних товарів. Імовірність неправомірного використання інформації дуже висока і збільшується через адміністративні рішення або комерційні операції» [8].

Особливо ці загрози актуалізувались для України у зв'язку з повномасштабним вторгненням рф, коли інформація у цифровому просторі туристичної галузі стала об'єктом інтересів не лише шахраїв та кіберзлочинців, але й спецслужб ворога. Це потребує кардинальної зміни ставлення до питань інформаційної безпеки та управління ризиками з боку усіх суб'єктів туристичної галузі, особливо тих, що у своїй діяльності послуговуються технологіями та інформаційною базою Smart-туризму чи забезпечують їх функціонування.

Слід зазначити, що теоретичне осмислення категорії «інформаційна безпека» ускладняється наявністю різних підходів до її визначення. Так, в одних наукових дослідженнях інформаційна безпека розглядається як процес, функція, діяльність, в інших – як стан, властивість інформаційного середовища, система гарантій [9]. Зокрема А.Ю. Нашинець-Наумова наводить близько 12-ти існуючих визначень інформаційної безпеки [10]. Смотрич Д.В. та Браілко Д.В. розглядає інформаційну безпеку в контексті протидії інформаційному впливу агресора на людську свідомість, що є елементом гібридної війни і здійснюється з метою дезорієнтації суспільства, залякування та маніпулювання суспільною думкою. При цьому її забезпечення розуміється як протидія інформаційним атакам ботів, а також фейкам [11].

Якщо говорити про інформаційну безпеку (Information Security) в контексті концепції «Smart-туризму» найбільш релевантним видається визначення, що міститься в Економічному енциклопедичному словнику, де вона трактується і як «стан захищеності систем обробки та зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації», і як «комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи знищення» [12].

При цьому, під цілісністю інформації мається на увазі її властивість «залишатися незмінною, в її первісному вигляді, структурі, під час її зберігання або багаторазової передачі». Її доступність передбачає, що «інформаційні дані, що знаходяться у вільному доступі, оперативно надаються легальним користувачам, без будь-яких зволікань і перешкод. Конфіденційність інформації базується на понятті створення обмеженого доступу до інформаційних ресурсів третіх, сторонніх осіб» [13].

Часто поняття інформаційна безпека ототожнюється з поняттями «кібербезпека» та «комунікативна безпека», що потребує уточнення. Кібербезпека передбачає забезпечення безпеки лише цифрової інформації, систем чи мереж від кіберзагроз, таких як хакерські атаки, віруси, несанкціонований доступ тощо. Об'єктом інформаційної безпеки в Smart-туризмі є інформація в будь-якій формі та на усіх її носіях. Вона спрямована, крім забезпечення кібербезпеки, на усунення широкого спектру загроз, зокрема загрози

фізичній безпеці носіїв інформації, несанкціонованого доступу до них, її поширення, зміни, знищення. Отже кібербезпеку можна вважати спеціалізованим напрямком забезпечення інформаційної безпеки. Відповідно, поняття «інформаційна система», в цьому контексті, це не лише цифрова, електронна система, воно має ширше значення.

Забезпечення інформаційної безпеки відбувається на усіх фазах її життєвого циклу (збору і створення, зберігання, передачі, обробки і використання, знищення або архівування). Комунікаційна безпека зосереджується на захисті інформації лише під час її передачі. Інформаційна безпека передбачає її захист на усіх етапах її життєвого циклу, від створення до утилізації.

Слід зазначити, що Smart-туризм базується на збиранні, обробці, аналізі і використання інформації, яка стосується, насамперед:

- персональних даних клієнтів та персоналу: ПІБ, адрес, номерів телефонів, електронних адрес, інформації про громадянство, номерів паспортів тощо.
- фінансової інформації: фінансового стану клієнтів (який опосередковано можна визначити на основі їх витрат в закладах гостинності), платіжних даних, реквізитів тощо.
- комерційної інформації: стратегічних планів підприємства туристичної галузі, списків клієнтів, комерційних таємниць.
- медичної інформації (якщо йдеться про рекреаційні заклади гостинності): медичні записи, історії хвороби, результати діагностики тощо.
- інтелектуальної власності: патентів, авторських прав, винаходів, ноу-хау тощо.
- інформації про клієнтів: звички, періодичність відвідування закладу, споживчі вподобання тощо.
- інфраструктури інформаційних систем: баз даних, програмного та апаратного забезпечення тощо [8].

В умовах воєнного стану уся ця інформація може представляти інтерес для ворога та бути використаною при плануванні терористичної атаки на об'єкт туристичної інфраструктури чи територію, де він знаходиться, призвести до руйнувань, загибелі людей, шантажу і вербування українців його спецслужбами. Особливо це актуально у зв'язку зі зміною контингенту закладів гостинності під час війни. Часто вони є прихистком для внутрішньо переміщених осіб, місцем розташування представників сектору оборони, волонтерів, журналістів, керівників органів влади та інших осіб, кого рф може вважати воєнною ціллю. Наслідком неналежного інформаційного захисту можуть бути також репутаційні та фінансові втрати як для окремих суб'єктів Smart-туризму, так і усієї вітчизняної туристичної галузі [14].

Першочерговим завданням на шляху забезпечення інформаційної безпеки в Smart-туризмі є виявлення причин несанкціонованого доступу до інформації, оцінка загроз для інформаційної безпеки його суб'єктів та створення потужних систем її захисту. Хоча, як свідчать дослідження проведені в Україні ще у довоєнний період, близько 80% зловмисників належить до офсайдерів [15], це не применшує ролі внутрішніх джерел витоку (навмисного чи ненавмисного) інформації. Її причиною може стати, зокрема, використання незахищених каналів зв'язку, наприклад, загальнодоступних мереж Wi-Fi в закладах гостинності, месенджерів з незашифрованим обміном повідомленнями тощо. Для отримання доступу до конфіденційних даних шахраями та ворогом можуть використовуватись соціально-інженерні технології, такі, наприклад, як «фішинг». Він передбачає надсилання повідомлення чи посилання, яке може стати причиною несанкціонованого доступу до персональних та фінансових даних, облікових даних доступу тощо. Персонал та гості можуть також їх втратити чи передати доступ третім особам. Небезпеку для інформаційної системи, можуть створювати їх пристрої, заражені зловмисними програмами. Підключившись до Wi-Fi закладу гостинності, чи до його цифрової інфраструктури, вони здатні передавати вірус в інформаційну систему, що може призвести до дуже важких наслідків. Наприклад, шпигунське програмне забезпечення здатне передавати зловмисникам інформацію про натискання клавіш, робити знімки екрана та застосовувати інші механізми стеження.

Слід зазначити, що ворог може отримати потрібну йому інформацію про, наприклад, місцезнаходження особи, що є об'єктом стеження, про переміщення та соціальні взаємодії також із відкритих джерел, зокрема з соціальних мереж персоналу чи гостей (наприклад, публікацій у Facebook або Twitter, відгуків на Booking або TripAdvisor, записів в блогах, розміщених фотографій тощо) [16]. Джерелом такої інформації може стати також несанкціонований доступ до записів з камер відеоспостереження.

Особливо небезпечно, коли дії щодо зміни, знищення чи передавання стороннім особам конфіденційної інформації здійснюється зовнішніми чи внутрішніми зловмисниками цілеспрямовано. Виявити небезпечні інциденти в цьому випадку – набагато важче [17]. В умовах війни це особливо актуалізує необхідність системної роботи кожного суб'єкта, що працює з інформацією, на якій базується Smart-туризм, над створенням та вдосконаленням комплексної системи захисту інформації, а з боку держави - постійного контролю та регулювання цього процесу.

Слід зазначити, що питання забезпечення захисту інформації в інформаційно-комунікаційних системах в Україні регламентуються рядом Законів: «Про інформацію» [18], «Про захист інформації в інформаційно-комунікаційних системах» [19], «Про захист персональних даних» [20] тощо. До деяких з них

було внесено відповідні зміни після повномасштабного вторгнення, існує ряд інших нормативних документів в галузі захисту інформації та державні стандарти України (ДСТУ) у цій сфері. 24 березня 2022 Верховною Радою України було ухвалено Закон від № 2160-IX «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому розповсюдженню інформації про направлення, переміщення міжнародної військової допомоги в Україну, рух, переміщення або розміщення Збройних Сил України чи інших військових формувань України, вчинене в умовах воєнного або надзвичайного стану», яким за ці дії передбачалась кримінальна відповідальність, з 2003 р. діє кримінальна відповідальність «за незаконне втручання в роботу комп'ютерів і комп'ютерних мереж, поширення комп'ютерних вірусів, якщо це призвело до спотворення, зникнення, блокування інформації чи її носіїв» [19]. Однак, як свідчить практика, не всі туристичні підприємства приділяють належну увагу питанням інформаційної безпеки. Причинами, з одного боку, є недостатнє усвідомлення користувачами інформаційних технологій їх значення та недооцінка загроз, з іншого - прагнення економії. Як результат, малі та середні підприємства галузі переважно не мають спеціалізованих підрозділів з інформаційної безпеки. Ці функції, в кращому випадку, доручаються системним адміністраторам або фахівцям відділу технічної підтримки, яким однак може бракувати кваліфікації з цих питань, або достатніх ресурсів. Фізичні особи, що працюють у сфері гостинності, взагалі перебувають поза зоною державного регулювання та контролю і часто необізнані з вимогами законодавства та не мають відповідної технічної бази для його дотримання. Однак реалії сьогодення вимагають від кожного суб'єкта туристичної сфери побудови комплексної системи інформаційної безпеки (рис. 3).

Для побудови та управління комплексною системою інформаційної безпеки необхідно здійснити оцінку ризиків з метою їх подальшого управління. Перш за все, потрібно визначити, які види інформації в обов'язковому порядку потребують захисту (це, наприклад, персональні дані гостей і персоналу, фінансова інформація, відомості про інфраструктуру інформаційної мережі тощо) та до яких наслідків може призвести її втрата, пошкодження чи зміна. Оцінити рівень безпеки інформаційних мереж можна за допомогою сучасного методу – пентесту. Його суть полягає в перевірці безпеки системи на предмет можливості проникнення та визначення вразливих місць у ній. Наприклад, в сфері кібербезпеки, за попередньою домовленістю з власником, інсценується атака кібер-шахраїв, які намагаються зламати систему, тим самим виявляючи її слабкі місця та вади. Однак цей підхід може використовуватись відносно усіх елементів системи безпеки інформації, стосовно усіх видів інформації та даних.

Рис. 3. Елементи комплексної системи інформаційної безпеки

Джерело: складено авторами

Важливим кроком в напрямку створення та управління комплексною системою інформаційної безпеки є розробка політики інформаційної безпеки, яка містить правила й процедури захисту інформації та роботи інформаційної інфраструктури, вимоги до персоналу та заходи з його перевірки на чесність та лояльність [21]. Її зміст має бути доведеним до відому кожного працівника (насамперед до тих, хто має доступ до конфіденційної інформації), періодично переглядатись та вдосконалюватись, з огляду на появу нових загроз та викликів у цій сфері. Персонал потрібно постійно навчати правилам і регламентам, зокрема адекватному реагуванню на соціально-інженерні атаки, на неправомірні дії інших осіб (зокрема колег та клієнтів) щодо конфіденційної інформації. Бажано створювати анонімні канали для повідомлення про такі дії тощо.

Важливою умовою управління дієвої системи інформаційної безпеки є оснащення інформаційної системи відповідними технічними засобами (наприклад, брандмауерами останнього покоління, антивірусним програмним забезпеченням, системами шифрування конфіденційної інформації та виявлення вторгнень в інформаційну мережу тощо). Звичайно, ці інструменти потребують значних витрат, але вони неспівставні з тими, що можуть бути у разі несанкціонованого доступу зловмисників до неї, DDoS-атаки на

сайт, витоку інформації, її втрати чи пошкодження. Ці витрати потрібно сприймати як інвестиції у власний стабільний розвиток та конкурентоспроможність.

Комплексна система інформаційної безпеки передбачає постійний моніторинг, спрямований на виявлення незвичайної активності, інцидентів, що несуть загрозу та вчасне реагування на них за визначеними заздалегідь протоколами. Зазначені вище заходи можуть носити разовий характер (наприклад у випадку перегляду прийнятих раніше рішень); здійснюватися лише у разі виникнення потреби (наприклад, у разі кадрових змін, придбання нового обладнання для обробки закритої інформації чи відповідних програм тощо), періодично (наприклад у в процесі впровадження, або виникнення певних змін в автоматизованій системі чи в зовнішньому середовищі; постійно (безперервно, або дискретно) [9, с. 211].

Слід зазначити, що маркетингова стратегія забезпечення інформаційної безпеки в Smart-туризмі значною мірою полягає в протистоянні загрозам, що виникли через появу новітніх IT технологій, які, з одного боку несуть благо для суспільства та галузі, а з іншого - надають додаткові можливості зловмисникам. Це, насамперед, Інтернет речей, технології 5D, квантові обчислення, штучний інтелект, хмарні технології тощо. Так, зростання кількості пристроїв, що працюють на базі Інтернету речей, розширення їх периферійної мережі та використання хмарних екосистем полегшує зловмисникам кібератаки. Квантові обчислення та комп'ютери, що працюють на їх основі, допомагають зламувати існуючі методи шифрування. Те саме стосується штучного інтелекту, який також може допомагати зловмисникам в проникненні, створювати зловмисні програми тощо.

Однак, слід зазначити, що в перспективі наведені технології можуть також використовуватись і для попередження, виявлення та ліквідації інформаційних небезпек. У зв'язку з значним збільшенням загроз під час війни в Україні та через швидке старіння будь-яких безпекових заходів, популярності набувають, крім традиційних інструментів інформаційної безпеки, модель «нульової довіри» та поведінкової біометрії.

Модель нульової довіри передбачає відмову від принципу «довіри за замовчуванням» («презумпції довіри») щодо кожного суб'єкта, що має до неї санкціонований доступ, та кожного пристрою, незалежно від того, всередині, чи за межами суб'єкта інформаційного захисту вони знаходяться. Передбачається, що захист вибудовується не лише по периметру інформаційної системи, але й усередині неї, на засадах безперервного моніторингу довіри, зокрема, поведінки людини та стану пристрою в реальному часі. Основними компонентами моделі нульової довіри є передові методи автентифікації, цілодобовий моніторинг і надійне шифрування, з відповідним коригуванням доступу.

Поведінкова біометрія базується на аналізі поведінки людини. При цьому аналізуються специфічні для користувачів характеристики такі як: «мова тіла», ритм набору тексту та рухи миші, особливості торкання до сенсорного екрану, манера тримання гаджета тощо. Це, звичайно не може замінити традиційні методи автентифікації (статичні облікових дані, такі як паролі, парольні фрази або PIN-коди), але цілком може їх доповнити [16]. Головний принцип – системна, комплексна робота над завданнями інформаційної безпеки, її багаторівневість та постійне вдосконалення.

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Smart-туризм, розвиток якого в світі та в Україні лише набирає темпу, створюючи значні вигоди для мандрівника, підприємств туристичної сфери та місцевих громад, при неналежному ставленні до питань інформаційної безпеки, може стати для даних суб'єктів джерелом значних ризиків, які потребують управління, розробки маркетингової стратегії та поетапного плану заходів. Особливо ця проблема актуалізується під час російсько-української війни, насамперед, після повномасштабного вторгнення. Інформація, яка акумулюється, обробляється та циркулює в інформаційній системі туристичної галузі та суб'єктів Smart-туризму може опинитись у руках ворога, бути зміненою, викраденою, знищеною, використовуватись в ході планування збройного та терористичного нападу, або кібератаки.

Ракетні атаки на заклади гостинності, кібератаки на туристичні сайти та цифрові платформи, що мали місце після початку повномасштабної війни, свідчать, що питанням інформаційної безпеки в туристичній галузі не приділяється належна увага, внаслідок чого вона несе іміджеві, матеріальні та фінансові втрати.

Питання забезпечення інформаційної безпеки у вітчизняні туристичній галузі та для суб'єктів туристичної сфери, що працюють з використанням Smart-технологій має стати об'єктом державного регулювання і контролю. Захист має здійснюватися на усіх етапах життєвого циклу інформації, з урахуванням новітніх тенденцій і явищ в сфері розвитку цифрових технологій. Перспективним напрямом забезпечення інформаційної безпеки, крім традиційних інструментів виявлення загроз, все більшого поширення набуває модель «нульової довіри» та поведінкова біометрія. Система інформаційної безпеки повинна носити комплексний характер, з застосуванням сучасних підходів, технічного оснащення та технологій. Її побудова не має бути разовим проєктом. Вона вимагає постійної кропіткої роботи та інвестицій. Подальшого вивчення вимагає дослідження стану реалізації принципів інформаційної безпеки вітчизняними закладами гостинності, що включені в інформаційну систему Smart-туризму, що планується дослідити в наступних роботах авторського колективу.

Література

1. Gretze1 U., Sigala M., Xiang Z., Koo C. Smart tourism: foundations and developments. *Electronic Markets*. August. 2015. P. 45-57. URL: https://www.researchgate.net/publication/280719315

2. Воронкова В.Г., Череп А.В. Креативні цифрові технології як мегатренди розвитку туристичного бізнесу: поширення європейського досвіду в Україні. *Humanities Studies*. 2020. Випуск 6(83). С. 163-179.

3. Воскресенська О.Є., Зінов`єва І.С. Розвиток SMART-туризму: теорія та практика. *Вісник ХНТУ*. 2020. № 3(74). С. 223-231.

4. Leading Examples of Smart Tourism Practices in Europe from the 2023 European Capital of Smart Tourism competition. European Capital and Green Pioneer of Smart Tourism. 2023, European Commission. 72 p. URL: https://smart-tourism-capital.ec.europa.eu/leading-examples-smart-tourism-practices-europe_en

5. Study on Mastering data for tourism by EU destinations / Galasso G. and other. Luxembourg: Publications Office of the European Union, 2022. 152 p. URL: https://op.europa.eu/en/publication-detail/-/publication/9df86541-fba5-11ec-b94a-01aa75ed71a1/language-en

6. From Smart Cities to Smart Tourism. Intellias. October 04, 2023. URL: https://intellias.com/from-smart-cities-to-smart-tourism/

7. Руденко М.В., Кирилюк Є.М., Хуторна М.Е. Цифровізація: маркетингові тренди та платформи реалізації. *Науковий вісник Одеського національного економічного університету*. 2022. № 5-6 (294-295), С. 80-88.

8. Дячек О.Ю., Рябченко К.М., Доценко А.В. Безпека даних в інформаційно-комунікаційному середовищі та її складність для нових бізнес-моделей. *Економіка та суспільство*. 2022. Вип. 38. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1273/1227

9. Маркіна, І.А., Гарічев Ю.М. Інформаційна безпека підприємства та організаційні заходи її забезпечення. *Український журнал прикладної економіки*. 2019. Том 4. № 4. С. 209–215.

10. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. К.: Видавничий дім «Гельветика», 2017. 168 с.

11. Смотрич Д.В., Браілко Л.В. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського НУ*. 2023 . Випуск 77. Ч. 2. С. 121-127.

12. Інформаційна безпека. Економічний енциклопедичний словник. URL: http://zalik.org.ua/index.php?newsid=25011

13. Інформаційна безпека: види загроз і методи їх усунення. DATAMI. 8 вересня 2020 URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/

14. Harrington D. Data Security: Definition, Explanation and Guide: Varonis / Inside Out Security Blog. July 6, 2021. URL: https://www.varonis.com/blog/data-security/

15. Коваленко Ю.О. Забезпечення інформаційної безпеки на підприємстві. *Економіка промисловості*. 2010. № 3. С. 123–129.

16. Masseno M., Santos C. Assuring Compliance of European Smart Tourist Destinations with the Principles of the General Data Protection Regulation: a roadmap. *Anuário da Proteção de Dados*. 2019. P. 87-108.

17. Kochuma I. Determinants of social policy in the formation of the human development institutional environment: management aspect. *Financial space*. 2020. № 4(40). P. 9-22.

18. Про інформацію: Закон України від 02 жовтня 1992 р. № 2657-XII від 02.10.1992 № 2657-XII. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

19. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 2 серпня 1994 р. N 18/94-ВР. URL: https://ips.ligazakon.net/document/Z008000

20. Про захист персональних даних: Закон України від 01 червня 2010 р. № 2297-VI. Відомості Верховної Ради України (ВВР), 2010, № 34, ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

21. Пантєлєєва Н.М. Цифрова економіка як ключовий тренд розвитку постіндустріального суспільства: монографія / за ред. Н.М. Пантєлєєвої, С.Ю. Колодія, М.А. Ребрика. К.: ДВНЗ «Університет банківської справи», 2019. 299 с.

References

1. Gretze1, U., Sigala, M., Xiang, Z., Koo, C. (2015). Smart tourism: foundations and developments. Electronic Markets. August. 45-57. URL: https://www.researchgate.net/publication/280719315.

2. Voronkova, V.G., Cherep, A.V. (2020). Kreatyvni tsyfrovi tekhnolohiyi yak mehatrendy rozvytku turystychnoho biznesu: poshyrennya yevropeys'koho dosvidu v Ukrayini [Creative digital technologies as megatrends in the development of tourism business: the spread of European experience in Ukraine]. Humanities Studies. 6(83),163-179.

3. Voskresenska, O.E., Zinov'eva, I.S. (2020) Rozvytok SMART-turyzmu: teoriya ta praktyka [Development of SMART tourism: theory and practice]. KhNTU Bulletin. 3(74), 223-231.

4. Leading Examples of Smart Tourism Practices in Europe from the 2023 European Capital of Smart Tourism competition. (2023). European Capital and Green Pioneer of Smart Tourism. 2023, European Commission. 72 p. URL: https://smart-tourism-capital.ec.europa.eu/leading-examples-smart-tourism-practices-europe_en.

5. Galasso, G. (2022). Study on Mastering data for tourism by EU destinations. Publications Office of the EU. URL: https://op.europa.eu/en/publication-detail/-/publication/9df86541-fba5-11ec-b94a-01aa75ed71a1/language-en.

6. From Smart Cities to Smart Tourism (2023). Intellias. October 04, 2023. URL: https://intellias.com/from-smart-cities-to-smart-tourism/

7. Rudenko, M.V., Kirilyuk, E.M., Khutorna, M.E. (2022). Tsyfrovizatsiya: marketynhovi trendy ta platformy realizatsiyi [Digitization: marketing trends and implementation platforms]. Naukovyy visnyk Odes'koho natsional'noho ekonomichnoho universytetu. 5-6 (294-295), 80-88.

8. Dyachek, O.Yu., Ryabchenko, K.M., Dotsenko, A.V. (2022). Bezpeka danykh v informatsiyno-komunikatsiynomu seredovyshchi ta yiyi skladnist' dlya novykh biznes-modeley [Data security in the information and communication environment and its complexity for new business models]. Ekonomika ta suspil'stvo. 38. URL: https://economyandsociety.in.ua/index.php/journal/article/view/1273/1227

9. Markina, I.A., Harichev, Yu.M. (2019). Informatsiyna bezpeka pidpryyemstva ta orhanizatsiyni zakhody yiyi zabezpechennya [Enterprise information security and organizational measures to ensure it]. Ukrayins'kyy zhurnal prykladnoyi ekonomiky. Vol. 4, 209–215.

10. Nashinets-Naumova, A.Yu. (2017). Informatsiyna bezpeka: pytannya pravovoho rehulyuvannya [Information security: issues of legal regulation] monograph. K.: Helvetica Publishing House.

11. Smotrych, D.V., Brailko, L.B. (2023). Informatsiyna bezpeka v umovakh voyennoho stanu [Information security in the conditions of martial law]. Naukovyy visnyk Uzhhorods′koho NU. 77(2), 121-127.

12. Informatsiyna bezpeka [Informational security]. Economic encyclopedic dictionary. URL: http://zalik.org.ua/index.php?newsid=25011.

13. Informatsiyna bezpeka: vydy zahroz i metody yikh usunennya [Information security: types of threats and methods of their elimination] (2020).URL: https://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/

14. Harrington, D. (2021). Data Security: Definition, Explanation and Guide: Varonis / Inside Out Security Blog. URL: https://www.varonis.com/blog/data-security.

15. Kovalenko, Yu.O. (2010). Zabezpechennya informatsiynoyi bezpeky na pidpryyemstvi [Ensuring information security at the enterprise]. Ekonomika promyslovosti. 3, 123–129.

16. Masseno, M., Santos, C. (2019). Assuring Compliance of European Smart Tourist Destinations with the Principles of the General Data Protection Regulation: a roadmap. Anuário da Proteção de Dados. 87-108.

17. Kochuma, I. (2020). Determinants of social policy in the formation of the human development institutional environment: management aspect. Financial space. 4(40), 9-22.

18. About information: Law of Ukraine dated October 2, 1992 No. 2657-XII dated October 2, 1992 No. 2657-XII. VVR, 1992, No. 48, Article 650. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

19. On the protection of information in information and communication systems: Law of Ukraine dated August 2, 1994 N 18/94-BP. URL: https://ips.ligazakon.net/document/Z008000.

20. On the protection of personal data: Law of Ukraine dated June 1, 2010 No. 2297-VI. Information of the VVR, 2010, No. 34, Art. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text.

21. Panteleeva, N.M. (2019). Tsyfrova ekonomika yak klyuchovyy trend rozvytku postindustrial'noho suspil'stva [Digital economy as a key trend in the development of post-industrial society] monograph. K.: University of Banking.