більшої кількості міжнародних мандрівників; запровадження передового світового досвіду організації бізнесу в туризмі; посилення євроінтеграційних процесів. Транскордонне співробітництво з європейськими країнами є перспективним стратегічним напрямком для реалізації концепції сприятливого, ефективного, безпечного туристичного відпочинку. Відновлення стратегічного потенціалу України і його перспективи розвитку є обґрунтованими відносно зміцнення співробітництва з країнами Близького Сходу і Азії. Важливо спростити візові формальності з групою країн. Полегшення процедури в'їзду та отримання віз сприятиме зростанню обсягів міжнародних прибуттів в Україну.

Література:

1. Tsviliy S.M., Ogloblina V.O., Demko V.S., Pavliuk A.A., Pisetskyi M.M. (2023). Potential of international cooperation of Ukraine in the geoeconomic space of the tourist industry. *GeoJournal of Tourism and Geosites*, no. 49(3), pp. 946-961.

2. Трусова Н.В., Цвілий С.М. Стійкий безпечний інноваційний розвиток у вітчизняній територіальній туристичній дестинації. *Інтелект XXI. Науковий економічний журнал.* Київ : Національний університет харчових технологій; Одеса ВД «Гельветика». 2023. № 2. С. 42-50.

ІНФОРМАЦІЙНІ ТА СОЦІАЛЬНІ АСПЕКТИ БЕЗПЕКИ ТУРИЗМУ

Худавердієва В.А., кандидат економічних наук, доцент,
Державний біотехнологічний університет, м. Харків, Україна
ORCID ID: https://orcid.org/0000-0002-0100-5079
Онищук А.В., здобувач вищої освіти,
Державний біотехнологічний університет, м. Харків, Україна

У зв'язку зі швидким розвитком інформаційних технологій та формуванням сучасного інформаційного суспільства суттєво трансформуються також підходи до трактування інформаційної безпеки туризму. Акценти поступово зміщуються від глобального та державного до локального та індивідуального рівнях. Особливо актуальними напрямами наукових пошуків є забезпечення безпеки в контексті поширення мережі Інтернет, а також проблеми, пов'язані зі збиранням персональних даних та доступом до них. Конституція України визначає інформаційну безпеку однієї з найважливіших функцій держави та справи всього українського народу.

Туризм як об'єкт дослідження вітчизняної економічної науки соціалізація та «інформатизація» торкнулися дуже поверхово. Варто зауважити, що трактування безпеки туризму за останні десятиліття зазнало суттєвих змін: від більш менш пасивного фактора - до активного елементу туризму та імперативу здійснення туристичної діяльності [1]. В рамках такого трактування категорії безпеки туризму системоутворюючу роль відіграє поняття загрози, що розглядається як деструктивне явище (подія), яке може спричинити посилення регресивних тенденцій розвитку туристичної діяльності на всіх ієрархічних рівнях та для всіх суб'єктів. Незважаючи на дещо звужене розуміння суті досліджуваної категорії, власне такий комплексний підхід, може бути покладено в основу загальної концепції, яка розглядатиме безпеку туризму дуалістично – як ключову передумову розвитку туристичної діяльності та як важливий чинник функціонування регіональних суспільних систем. Справді, з огляду на важливу громадську роль туризму, і навіть вагомого впливу соціальних чинників на туристичну діяльність, підтвердженого низкою досліджень [2; 3], можемо констатувати, що категорія соціальної безпеки туризму має бути предметом сучасних наукових пошуків та потребує додаткового обґрунтування. Розглядати категорію соціальної безпеки туризму слід у рамках міждисциплінарних регіональних економічних досліджень безпеки туризму загалом. Отже, ґрунтуючись на підходах до трактування соціальної безпеки у вітчизняній економічній науці, сучасних тенденціях зарубіжних досліджень безпеки туризму, розглядати соціальну безпеку туризму у регіоні необхідно як стан функціонування регіональної туристичної системи, що характеризується захищеністю всіх її підсистем (туристів, туристичних підприємств та дестинацій) від зовнішніх та внутрішніх загроз соціального характеру, а також здатністю адекватно реагувати на виклики та забезпечувати формування сталого стратегічного потенціалу розвитку туризму в умовах соціалізації економіки регіону.

Розробляючи визначення інформаційної безпеки туризму, варто проаналізувати основні підходи у вітчизняній та зарубіжній науці до трактування поняття «інформаційна безпека» на різних рівнях (особистості, підприємства, суспільства). Загалом у вітчизняній науці поширений диференційований підхід до обґрунтування сутності інформаційної безпеки, який розглядає це поняття з різних точок зору залежно від об'єкта дослідження. Відповідно до розробленої класифікації безпеки туризму за змістом, виділяється дві основні складові інформаційної безпеки – безпеку персональних даних та

безпеку інформаційного середовища. Варто зауважити, що ці підсистеми інформаційної безпеки туризму тісно пов'язані між собою і, розглядаючи окремі аспекти туристичної діяльності, їх доцільно аналізувати тільки в комплексі [3]. Отже, в сучасних умовах здійснення туристичної діяльності соціальні та інформаційні проблеми безпеки туризму набувають все більшої актуальності. Враховуючи це, важливим завданням економічних досліджень безпеки туризму є обґрунтування їх теоретико-методологічних засад, насамперед щодо визначення ключових понять та структурних особливостей.

Проблема захисту від несанкціонованого доступу особливо загострилася з поширенням локальних і особливо глобальних комп'ютерних мереж. Необхідно також зазначити, що найчастіше шкода завдається не через «злий намір», а через елементарні помилки користувачів, які випадково псують або видаляють життєво важливі дані. У зв'язку з цим, крім контролю доступу, необхідним елементом захисту в комп'ютерних мережах є розмежування повноважень користувачів. У комп'ютерних мережах при організації контролю доступу та розмежування повноважень користувачів найчастіше використовуються вбудовані засоби мережевих операційних систем. Але в такій системі організації захисту все одно залишається слабке місце: рівень доступу та можливість входу до системи визначаються паролем. Для виключення можливості неавторизованого входу в комп'ютерну мережу останнім часом використовується комбінований підхід - пароль + ідентифікація користувача по персональному «ключу». В якості «ключа» може використовуватися пластикова карта (магнітна або з вбудованою мікросхемою – смарт-картка) або різні пристрої для ідентифікації особистості за біометричною інформацією – по райдужній оболонці ока або відбиткам пальців, розмірам кисті руки і т.д.

Оснастивши сервер або мережеві робочі станції, наприклад, пристроєм читання смарт-карток та спеціальним програмним забезпеченням, можна значно підвищити рівень захисту від несанкціонованого доступу. У цьому випадку для доступу до комп'ютера користувач повинен вставити смарт-картку в пристрій читання та ввести персональний код. Програмне забезпечення дозволяє встановити кілька рівнів безпеки, які управляються системним адміністратором. Можливий і комбінований підхід із введенням додаткового пароля, при цьому вжито спеціальних заходів проти «перехоплення» пароля з клавіатури. Цей підхід значно надійніший за застосування паролів, оскільки, якщо пароль підгледіли, користувач про це може не знати, якщо ж зникла картка, можна вжити заходів негайно.

Смарт-картки управління доступом дозволяють реалізувати, зокрема, такі функції, як контроль входу, доступ до пристроїв персонального комп'ютера, доступ до програм, файлів і команд.

Захист інформації під час віддаленого доступу: у міру розширення діяльності підприємств, зростання чисельності персоналу та появи нових філій виникає необхідність доступу віддалених користувачів (або груп користувачів) до обчислювальних та інформаційних ресурсів головного офісу компаній. У зв'язку з цим захист інформації, що передається каналами віддаленого доступу, вимагає особливого підходу. Зокрема, в мостах і маршрутизаторах віддаленого доступу застосовується сегментація пакетів - їх поділ і передача паралельно по двох лініях, - що унеможливлює «перехоплення» даних при незаконному підключенні «хакера» до однієї з ліній. До того ж використовується при передачі даних процедура стиснення пакетів, що передаються, гарантує неможливість розшифровки «перехоплених» даних. Крім того, мости та маршрутизатори віддаленого доступу можуть бути запрограмовані таким чином, що віддалені користувачі будуть обмежені у доступі до окремих ресурсів мережі головного офісу.

Розроблені й спеціальні пристрої контролю доступу до комп'ютерних мереж по комутованим лініям. Наприклад, фірмою AT&T ще в 1995 році був запропонований модуль Remote Port Security Device (PRSD), що представляє собою два блоки розміром зі звичайний модем: RPSD Lock (замок), що встановлюється в центральному офісі, і RPSD Key (ключ), що підключається до модему віддаленого користувача. RPSD Key і Lock дозволяють встановити кілька рівнів захисту та контролю доступу, зокрема: робочих місць (work location sub-system) і шифрування даних, що передаються по лінії за допомогою генерованих цифрових ключів. В даний час асортимент пропонованих на ринку додатків для обмеження доступу досить широкий і охоплює різноманітні програмні продукти. Одні з них блокують доступ до налаштувань операційної системи, інші – дозволяють контролювати доступ до різноманітних пристроїв, треті – повністю блокують комп'ютер без користувача, четверті – забезпечують приховування персональних даних. Нерідко зазначені можливості поєднуються в тій чи іншій комбінації, що цілком зрозуміло, адже багатьом користувачам для вирішення завдань, що стоять перед ними, потрібно обмежити доступ відразу по кількох напрямках [1].

Таким чином, вибір для конкретних інформаційних систем має бути заснований на глибокому аналізі слабких та сильних сторін тих чи

інших методів захисту. Обґрунтований вибір тієї чи іншої системи захисту, загалом, має спиратися на якісь критерії ефективності. На жаль, досі не розроблено відповідних методик оцінки ефективності криптографічних систем. Найбільш простий критерій такої ефективності – ймовірність розкриття ключа чи потужність безлічі ключів, інакше кажучи, криптостійкість. Для її чисельної оцінки можна використовувати також складність розкриття шифру шляхом перебору всіх ключів. Але в цій схемі є ряд недоліків, що визначаються тим, що цей критерій не враховує важливих вимог до криптосистем: неможливість розкриття або осмисленої модифікації інформації на основі аналізу її структури; досконалість використовуваних протоколів захисту; мінімальний обсяг використовуваної ключової інформації; мінімальна складність реалізації (у кількості машинних операцій), її вартість; висока оперативність.

Література:

1. Галатенко В.А. Категорування інформації та інформаційних систем. Забезпечення базового рівня інформаційної безпеки. Jet Info. 2022. № 4. URL: http://www.jetinfo./stati/kategorirovanie-informatsii-i-informatsionnykh (дата звернення: 29.02.2024).

2. Fuchs L. Roles in information security – A survey and classification of the research area. Computers & Security, 2017, vol. 30, issue 8. pp. 748-769. DOI: https://doi.org/10.1016/j.cose. 2017.08.002

3. Брюхомицький Ю.А., Макаревич О.Б. Огляд досліджень та розробок з інформаційної безпеки. За матеріалами доповідей XII Міжнар. наук.-практ. конф. «Інформаційна безпека – 2020». Вісті ЮФУ. Технічні науки. 2020. С. 8-21.

ТЕНДЕНЦІЇ РОЗВИТКУ УКРАЇНСЬКОГО ТУРИЗМУ В УМОВАХ ВІЙНИ

Червінська Т.М., кандидат економічних наук, доцент,
Київський університет інтелектуальної власності
та права НУ «Одеська юридична академія», м. Київ, Україна
ORCID ID: https://orcid.org/0000-0001-7657-2855

До пандемії коронавірусу й повномасштабного вторгнення рф, туристична сфера складала 2,3 % ВВП України й забезпечувала близько 375 тис. робочих місць. Але реальний внесок туризму в якість життя й добробут українців значно більший, адже його мультиплікативний ефект стимулює витрати в суміжних галузях: торгівлі, транспорті,