УДК 338.48.242(477)

М. В. Грабар,
к. е. н., доцент, доцент кафедри туризму,
ДВНЗ "Ужгородський національний університет"
ORCID ID: https://orcid.org/0000-0002-2753-4462
Г. В. Машіка,
д. геогр. н., професор, професор кафедри туризму,
ДВНЗ "Ужгородський національний університет"
ORCID ID: https://orcid.org/0000-0001-6063-5823
М. Ю. Кашка,
к. і. н., доцент, доцент кафедри туризму,
ДВНЗ "Ужгородський національний університет"
ORCID ID: https://orcid.org/0000-0001-7437-6156
О. В. Пригара,
к. б. н., доцент кафедри туризму,
ДВНЗ "Ужгородський національний університет"
ORCID ID: https://orcid.org/0000-0003-3433-7173

DOI: 10.32702/2306-6792.2023.3-4.43

КОНЦЕПТУАЛЬНІ ОСНОВИ КІБЕРБЕЗПЕКИ СФЕРИ ТУРИЗМУ ТА РЕКРЕАЦІЇ

M. Hrabar,
PhD in Economics, Associate Professor of the Department of Tourism,
Uzhhorod National University
H. Mashika,
Doctor of Science in Geography, Professor of the Department of Tourism,
Uzhhorod National University
M. Kashka,
PhD in History, Associate Professor of the Department of Tourism,
Uzhhorod National University
O. Pryhara,
PhD in Biology, Associate Professor of the Department of Tourism,
Uzhhorod National University

CONCEPTUAL BASICS OF CYBER SECURITY IN THE SPHERE OF TOURISM AND RECREATION

У статті досліджено концептуальні основи кібербезпеки сфери туризму та рекреації. Зазначено, що в епоху цифрової трансформації компанії в усіх галузях, як правило, стикаються з тими чи іншими порушеннями даних і конфіденційності. Охарактеризовано особливості технологічного простору кібербезпеки туризму. Проаналізовано наступні чинники, що впливають на функціонування туризму у кіберпросторі: складна структура власності, використання електронних методів оплати, обізнаність співробітників, сезонність роботи та плинність кадрів, регулярне технічне обслуговування та резервне копіювання систем, суверенітет даних і видалення даних, використання нових та інноваційних технологій. Висвітлено причини збільшення кібеатак, а саме: дефіцит кваліфікованих спеціалістів з кібербезпеки, перехід на дистанційну та гібридну роботу, зростання активності у даркнеті, поява нових тактик кібератак, інтерес до криптовалюти, активність програм-вимагачів, вплив віртуального світу.

The article examines the conceptual foundations of cyber security in the field of tourism and recreation. It is noted that in the era of digital transformation, companies in all industries, as a rule, face one or another breach of data and privacy. The peculiarities of the technological space of tourism cyber security are characterized. The following factors affecting the functioning of tourism in cyberspace were analyzed: complex ownership structure, use of electronic payment

Передплатний індекс 21847

methods, employee awareness, seasonality of work and staff turnover, regular maintenance and backup of systems, data sovereignty and data deletion, use of new and innovative technologies. The reasons for the increase in cyberattacks are highlighted, namely: the shortage of qualified cyber security specialists, the transition to remote and hybrid work, the growth of activity in the darknet, the emergence of new cyberattack tactics, interest in cryptocurrency, the activity of ransomware, and the influence of the virtual world. Because every travel company is unique, it faces its own spectrum of cybersecurity risks. A clear set of controls is vital to minimizing the likelihood of a personal data breach. Data leakage is considered one of the worst dangers that can damage a brand's reputation. It is estimated that around 87% of customers will leave and take their business elsewhere after a data breach. Therefore, it is important for companies to maintain a strong cybersecurity position. It is emphasized that it is difficult for travel companies to control the data of identification information, especially when it is important to share it with many suppliers (eg hotels, airlines). Also, travel companies often depend on the use and security of third-party reservation systems. At the same time, most travel companies are small and medium-sized enterprises without a dedicated cyber security team or information security manager. The tourism and leisure industry is highlighted as an ideal platform for cybercriminals looking to commit financial fraud and identity theft crimes. The importance of cyber security is evidenced at the state level, which is reflected in the Law of Ukraine "On the Basic Principles of Ensuring Cyber Security of Ukraine".

Ключові слова: туризм, рекреація, кібербезпека, кіберстійкість, дані, захист.
Key words: tourism, recreation, cyber security, cyber resilience, data, protection.

ПОСТАНОВКА ПРОБЛЕМИ

В епоху цифрової трансформації компанії в усіх галузях, як правило, стикаються з тими чи іншими порушеннями даних і конфіденційності. Сфера туризму та рекреації в цьому відношенні не є винятком, оскільки туристичні компанії, як правило, збирають і зберігають перевірені дані про клієнтів (зокрема офіційні імена, номери і серії паспортів, інформацію про кредитні картки). Це, у свою чергу, робить галузь ідеальною платформою для кіберзлочинців, які хочуть вчиняти фінансові шахрайства та злочини, пов'язані з крадіжкою особистих даних. Тому для туристичних компаній дуже важливо вжити належних заходів для забезпечення безпеки особистих та фінансових даних мандрівників. Забезпечення конфіденційності та безпеки таких даних може бути складним завданням, проте це невідмінна умова успішної взаємодії із клієнтами.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Кіберстійкість як основу національної безпеки України розглядали у своїй праці С. В. Онищенко, А. Д. Глушко, О. А. Маслій. Авторами здійснено ідентифікацію ризиків кібербезпеці України та проведено оцінюванню рівня кіберстійкості на основі даних міжнародних рейтингів [2, с. 551].

В. Ю. Биков, О. Ю. Буров, Н. П. Дементієвська досліджували кібербезпеку в цифровому навчальному середовищі. Акцентується проблематика стійкості до кібернебезпек, яка може використовувати досвід підготовки операторів емерджентних галузей, у тому числі діагностування поточного стану людини та необхідне коригування з метою оптимізації її діяльності [1, с. 313].

Ю. І. Хлапонін, Л. М. Козубцова, І. М. Козубцов, Р. М. Штонда характеризували функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. Запропоновано універсальні функції, які має реалізовувати система захисту інформації і кібербезпеки на об'єктах критичної інформаційної інфраструктури [4, с. 124].

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ (ПОСТАНОВКА ЗАВДАННЯ)

Метою роботи є дослідження кібербезпеки туризму та рекреації і виявлення особливостей та закономірностей функціонування галузі в кіберпросторі.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Значущість і важливість кібербезпеки посилюється зі зростанням важливості мережевих пристроїв, що стимулюється розвитком Індуст-

Передплатний індекс 21847

рії 4.0, тобто появою ризиків, пов'язаних з несанкціонованим доступом до інформації, що зберігається в базах даних, а також несанкціонованим захопленням контролю над роботою пристроїв [7, с. 76].

Ю. І. Хлапонін, Л. М. Козубцова, І. М. Козубцов, Р. М. Штонда під системою захисту інформації і кібербезпеки розуміють складний комплекс програмних, криптографічних, організаційних та інших засобів, методів і заходів призначених для захисту інформації та кібербезпеки [4, с. 125].

Згідно закону України "Про основні засади забезпечення кібербезпеки України" кібербезпека — це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1, с. 314].

Кібербезпека стала невідємною частиною усіх сфер бізнесу та приватного життя. Тому з боку державної влади налагоджені відповідні служби, що займаються питанням кібербезпеки. Зокрема, Державна служба спеціального зв'язку та захисту інформації України щоквартально подає інформацію про стан кібератак в Україні. У 3 кварталі 2022 р. за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд. подій інформаційної безпеки. Фахівці Державного центру кіберзахисту зафіксували істотне зростання розповсюдження шкідливого програмного забезпечення, яке дає можливість хакерам викрадати дані чи й взагалі знищувати їх. При цьому основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та знищення даних інформаційних систем. Порівняно з попереднім кварталом, кількість подій інформаційної безпеки з високим рівнем критичності зросла у 3,8 рази, кількість зареєстрованих кіберінцидентів із високим рівнем критичності зросла на 128% [3].

Згідно рейтингу NCSI — глобального індексу кібербезпеки у 2021 р. Україна посіла 24 місце серед 160 країн та поліпшила свою позицію на 1 пункт у порівнянні з 2020 р. В його основі закладено розрахунок 12 індикаторів, які засвідчують досягнення країни за такими напрямами: розробленість політики з кібербезпеки, моніторинг та аналіз кіберзагроз, освіта та підвищення кваліфікації у сфері кіберзахисту, внесок у глобальну кібербезпеку, захист цифрових сервісів, захист основних послуг у кіберпросторі, послуги електронної ідентифікації, захист персональних даних, реагування на кіберінциденти, кіберкризове управління, боротьба з кіберзлочинністю та військові кібероперації [2, с. 552].

Кібербезпеку слід розглядається як складну та багатопрофільну сферу, що потребує постійної уваги. Легко засудити туристичну компанію за слабкий контроль кібербезпеки та конфіденційності, але важливо враховувати контекст, у якому вона працює:

— дані ідентифікаційної інформації важко контролювати, особливо коли важливо поділитися ними з багатьма постачальниками (наприклад, готелями, авіакомпаніями та екскурсійними бюро);

— туристичні компанії часто залежать від використання та безпеки сторонніх систем бронювання;

— більшість туристичних компаній є малими та середніми підприємствами без спеціальної команди з кібербезпеки або керівника інформаційної безпеки.

Оскільки кожна туристична компанія унікальна, вона стикається з власним спектром ризиків кібербезпеки. Чіткий набір елементів керування є життєво важливим для мінімізації ймовірності порушення персональних даних.

Витік даних вважається однією із найгірших небезпек, що здатна завдати шкоди репутації бренду. За оцінками, близько 87 % клієнтів підуть і перенесуть свій бізнес в інше місце після витоку даних. Тому для компаній важлива підтримка міцної позиції кібербезпеки. На рис. 1 представлено складнощі технологічного простору кібербезпеки туризму. Проаналізуємо наведену схему.

Складна структура власності — часто підприємства туристичної індустрії (такі як готелі, ресторани та туристичні компанії) можуть мати складну структуру власності, яка включає керуючу компанію, яка керує бізнесом, окремого власника або групу власників і франчайзера. Ці окремі суб'єкти спільно працюють як команда, щоб взяти на себе різні обов'язки для забезпечення безперебійної роботи бізнесу. Ці об'єкти можуть зберігати важливі дані в різних системах, і такі дані можуть постійно переміщуватися. Коротше кажучи, ці складні структури власності можуть призвести до серйозних порушень даних.

Використання електронних методів оплати. Індустрія туризму значною мірою залежить від способів оплати онлайн. Для бронювання по-

Передплатний індекс 21847

Рис. 1. Особливості технологічного простору кібербезпеки туризму

Джерело: сформовано авторами.

трібно вказати дані кредитної картки, а платежі часто здійснюються тією ж карткою, яка вже зберігається, оскільки це зручно як для клієнтів, так і для працівників. Як тільки один файл у системі буде зламано, існує величезна ймовірність того, що вся колекція взаємопов'язаних пристроїв опиниться під загрозою. Режими онлайн-платежів можуть бути легкою мішенню для отримання ключової особистої та фінансової інформації. Туристичні та готельні компанії повинні забезпечити безпеку всіх пристроїв, які використовуються для зберігання фінансових даних клієнтів, за допомогою багатьох заходів, таких як система двофакторної автентифікації.

Обізнаність співробітників. Туристичні компанії повинні переконатися, що їхні співробітники вживають рішучих і адекватних заходів для захисту даних, які вони обробляють, використовуючи фільтр конфіденційності на ноутбуках, планшетах, сигналізація використання PIN, паролю, блокування для захисту від кіберзлочинів. Це допоможе захистити дані та забезпечити персональне дотримання вимог.

Сезонність роботи та плинність кадрів. Наявність добре навчених співробітників важлива для забезпечення безпечного збору та зберігання даних клієнтів і компанії. Однак індустрія туризму зазнає відносно високих загроз, оскільки вона в основному включає сезонну зайнятість, коли працівники часто залишають або переводяться в інші місця. Це ускладнює посилення команд належним чином підготовлених працівників. Насправді один ненавчений співробітник може надати кіберзлочинцям легкі лазівки для викрадення конфіденційних даних клієнтів.

Регулярне технічне обслуговування та резервне копіювання систем. Використання старих і застарілих систем програмного забезпечення дозволяє кіберзлочинцям легко викрасти дані або зламати систему. Тому важливо регулярно обслуговувати пристрої та оновлювати програмне забезпечення. Резервне копіювання даних, як правило, є простим і економічно ефективним способом забезпечення безпеки даних. Такі дані включають фінансові записи, бізнес-плани, дані клієнтів, особисту інформацію тощо.

Суверенітет даних і видалення даних. Суверенітет даних стосується прав на зберігання даних компанії та клієнтів на основі географічного положення. Різні закони, пов'язані з цим аспектом, діють для захисту даних і гарантують конфіденційність населення від зовнішніх загроз. Аспект суверенітету даних дає будь-якій компанії право оприлюднювати або приховувати будь-яку інформацію, яка зберігається в системі кібербезпеки. Більшість туристичних компаній не мають політики зберігання та утилізації конфіденційних даних клієнтів і електронної інформації, і це збільшує ризик витоку даних.

Використання нових та інноваційних технологій надає різноманітні можливості для посилення політики і стратегії конфіденційності та безпеки даних. Наприклад, блокчейн пропонує численні можливості для покращення управління подорожами та витратами. Від підтвердження особи, усунення незручних обмінів із паспортним контролем до програм лояльності та бонусів, це може допомогти забезпечити інформаційну безпеку. Подібним чином автоматизація за допомогою машинного навчання і штучного інтелекту також може виявитися корисною.

Проблеми безпеки даних стали справжнім викликом для бізнесу. Сучасні тенденції відоб-

Передплатний індекс 21847

Таблиця 1. Причини збільшення кібеатак

№	Назва	Характеристика
1	Дефіцит кваліфікованих спеціалістів з кібербезпеки	Згідно з дослідженням Cybersecurity Workforce Study, глобальна нестача кадрів у сфері кібербезпеки становить 3,4 млн осіб, при цьому 70% організацій мають незакриті вакансії.
2	Перехід на дистанційну та гібридну роботу	Кількість спроб атак на протокол віддаленого робочого столу (RDP) зросла на рекордні 768% протягом 2020 р., що виявилось одним із найуразливіших місць в інфраструктурі підприємств.
3	Зростання активності у даркнеті	Величезне зростання кримінальної активності у даркнеті за останні роки, особливо після початку пандемії, є серйозною проблемою, яка ще раз показує важливість досліджень у цих мережах Інтернету.
4	Поява нових витончених тактик кібератак	Одним із різновидів фішингу, який останнім часом активізувався, є гібридний фішинг, який поєднує традиційний метод на основі електронної пошти з вішингом.
5	Інтерес до криптовалюти	Використовуючи платформи у галузі криптовалют, NFT та ігор, зловмисники часто створюють нові фішингові сайти для викрадення облікових даних користувачів, зокрема для входу у криптовалютні гаманці.
6	Активність програм-вимагачів	З 2020 по 2021 рік кількість атак програм-вимагачів зросла удвічі, залишаючись найбільш руйнівною загрозою для підприємств.
7	Вплив віртуального світу	Прогнози щодо розвитку метавсесвіту показують, що до 2026 р. 25% населення світу проводитиме принаймні 1 годину на день у цьому віртуальному світі.
8	Недостатня обізнаність користувачів	Базова проблема, з якою кібербезпека завжди стикатиметься, це недостатня цифрова обізнаність працівників щодо векторів атак та способів їх розпізнання. Тому співробітники є найслабшою ланкою захисту будь-якої організації. Однак завдяки підвищенню обізнаності сучасним загрозам персонал може стати першою лінією кіберзахисту.

Джерело: сформовано на основі [6].

ражають негативний вплив всесвітньої пандемії, а статистика кібербезпеки демонструє значне зростання кількості витоків даних і хакерських операцій.

Однак, необхідно враховувати наступні принципи, щоб зменшити ризик витоку даних:

— пріоритет захисту CRM та систем бронювання. Такі системи зазвичай містять мільйони ідентифікаційних даних записів і, отже, мають займати перше місце в списку для оцінки ризиків і впровадження ефективних заходів безпеки;

— зведення до мінімуму даних, які збираються та передаються. Хоча це може здатися зручним для збору й обміну одними і тими самими клієнтськими даними з усіма постачальниками, це не обов'язково. Наприклад, чи потрібно оператору сафарі надсилати повні скани паспортів клієнтів перед поїздкою;

— зберігати дані ідентифікаційної інформації протягом необхідного періоду. Доцільно враховувати період, протягом якого дані ідентифікаційної інформації необхідні для ведення бізнесу та виконання нормативних вимог. Створення чіткої політики зберігання допоможе видалити дані, які більше не потрібні;

— зосередженя на контролі доступу. Оскільки більшість даних ідентифікаційної інформації тепер зберігаються в хмарних рішеннях, керування доступом стало новим обмеженням мережі. Почати доцільно із увімкнення 2FA для всіх облікових записів і спростити адміністрування за допомогою системи єдиного входу, де це можливо.

— відстеження та контроль використання Shadow IT. Як правило, туристичні компанії мають розгалужені відділи продажів і маркетингу, які схильні завантажувати дані в низку несхвалених онлайн-інструментів, таких як платформи аналізу даних.

Недотримання описаних принципів провокує зростання імовірності загрози кібербезпеці, що може завдати значної шкоди туристам. Ця шкода пов'язана із завантаженням інформації про банківські картки чи банківські рахунки, завантаженням персональних даних туристів та потенційним ризиком їх продажу на чорному ринку.

Відповідно до звіту Cybersecurity Ventures, очікується, що глобальні збитки, спричинені

Передплатний індекс 21847

кіберзлочинною діяльністю зростатимуть на 15% з 2021 до 2025 р. та можуть досягти 10,5 трлн дол. США щорічно [5].

ESET — глобальна компанія у сфері захисту від кіберзлочинності та цифрових загроз акцентує увагу на наступних основних викликах, які постають перед кібербезпекою (табл. 1).

Таким чином, дослідивши кібербезпеку туризму можемо констатувати:

— кібербезпека визначається як область, пов'язана з обчислювальною технікою та телематикою, яка зосереджена на захисті комп'ютерної інфраструктури та уникненні всіх видів загроз, які ставлять під загрозу інформацію, яка обробляється, транспортується та зберігається на будь-якому пристрої;

— вагомість кібербезпеки засвідчується на державному рівні, що має свій прояв у законі України "Про основні засади забезпечення кібербезпеки України". Контроль та реагування на кіберінциденти та кібератаки здійснюється Державною службою спеціального зв'язку та захисту інформації України;

— кібербезпека туризму повязана із специфікою цього бізнесу, зокрема дані ідентифікаційної інформації важко контролювати, особливо коли важливо поділитися ними з багатьма постачальниками; туристичні компанії часто залежать від використання та безпеки сторонніх систем бронювання. При цьому більшість туристичних компаній є малими та середніми підприємствами без спеціальної команди з кібербезпеки або керівника інформаційної безпеки.

Література:

1. Биков В.Ю., Буров О.Ю., Дементієвська Н.П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології та засоби навчання. № 2(70). 2019. С. 313—331.

2. Онищенко С.В., Глушко А.Д., Маслій О.А. Кіберстійкість як основа національної безпеки України. Proceedings of XI International Scientific and Practical Conference "Innovations and prospects of world science" (Vancouver, Canada, 22—24 June 2022). Vancouver: Perfect Publishing, 2022. — P. 551—556.

3. Служба безпеки України. Захист інформаційного та кіберпростору. Звіт SIEM. URL: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (дата звернення 11.01.2023).

4. Хлапонін Ю. І., Козубцова Л. М., Козубцов І. М., Штонда Р. М. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури. Кібербезпека: освіта, наука, техніка. № 3 (15), 2022. С. 124—134. DOI 10.28925/2663-4023.2022.15.1241341

5. Cybersecurity Ventures Cybercrime To Cost The World $10.5 Trillion Annually By 2025. URL: https://cybersecurityventures.com/(дата звернення 17.01.2023).

6. ESET. 10 викликів кібербезпеки: до чого готуватися користувачам та компаніям. URL: https://www.eset.com/ua/about/ (дата звернення 15.01.2023).

7. Kovacic M., Cicin-sain M., Milojica V. Cyber security and tourism: bibliometric analysis. Journal of Process Management and New Technologies. Vol. 10, Issue 3—4, 2022, pp. 75—92.

References:

1. Bykov, V.Iu., Burov, O.Iu. and Dementiievska, N.P. (2019), "Cyber Security in a Digital Learning Environment", Informatsiini tekhnolohii ta zasoby navchannia — Information Technologies and Learning Tools, vol. 70 (2), pp. 313—331.

2. Onyshchenko, S.V., Hlushko, A.D. and Maslii O.A. (2022), "Cyber resilience as the basis of Ukraine's national security", Innovations and prospects of world science. Proceedings of XI International Scientific and Practical Conference "Innovations and prospects of world science", Perfect Publishing, Vancouver, Canada, 22—24 June, pp. 551—556.

3. Security Service of Ukraine (2022), "Protection of information and cyberspace. SIEM report", available at: http://ssu.gov.ua/zabezpechennia-informatsiinoi-bezpeky (accessed 11 January 2023).

4. Khlaponin, Yu. I., Kozubtsova, L. M., Kozubtsov, I. M. and Shtonda R. M. (2022), "Functions of the information protection system and cyber security of critical information infrastructure", Kiberbezpeka: osvita, nauka, tekhnika — Cyber security: education, science, technology, vol. 3 (15), pp. 124—134. DOI 10.28925/2663-4023.-202215.1241341(in Ukrainian).

5. Cybersecurity Ventures (2022), "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", available at: https://cybersecurityventures.com/ (accessed 17.01.2023).

6. ESET (2022), "10 cyber security challenges: what users and companies should prepare for ", available at: https://www.eset.com/ua/about/ (accessed 15.01.2023).

7. Kovacic, M., Cicin-sain, M. and Milojica V. (2022), "Cyber security and tourism: bibliometric analysis", Journal of Process Management and New Technologies, vol. 10, Issue 3-4, pp. 75—92.

Стаття надійшла до редакції 25.01.2023 р.

Передплатний індекс 21847