УДК 640.4:659.126]:004.946.5.056
DOI: 10.31866/2616-7468.5.2.2022.270089

# КІБЕРЗАХИСТ готельних брендів

***Ірина Верезомська,***
*кандидатка економічних наук,*
*Київський національний університет культури і мистецтв,*
*Київ, Україна,*
*verez_kult@ukr.net*
*https://orcid.org/0000-0002-3289-3734*
*© Верезомська І., 2022*

***Людмила Бовш,***
*кандидатка економічних наук,*
*Державний торговельно-економічний університет,*
*Київ, Україна,*
*l.bovsh@ukr.net*
*https://orcid.org/0000-0001-6044-3004*
*© Бовш Л., 2022*

***Ксенія Приходько,***
*викладачка,*
*Київський національний університет культури і мистецтв,*
*Київ, Україна,*
*prykhodko11@ukr.net*
*https://orcid.org/0000-0002-7347-3226*
*© Приходько К., 2022*

***Христина Баклан,***
*магістрантка,*
*Київський національний університет культури і мистецтв,*
*Київ, Україна,*
*gajtynka@ukr.net*
*https://orcid.org/0000-0002-7574-5870*
*© Клименко Х., 2022*

**Актуальність.** Готельна сфера зазнала значних фінансових потрясінь під час пандемії, які загострились в умовах військового стану в Україні. Актуальною стала проблематика захисту нематеріальних активів, зокрема в умовах, коли деякі вітчизняні готелі мають російських бенефіціарів та певні міжнародні бренди лишились працювати в Росії, що розв'язала повномасштабну війну в Україні. Крім фізичного знищення, готелі стали також предметом інформаційної війни та кіберзлочинів. Тому питання кіберзахисту брендів стали важливою складовою стратегії розвитку, зокрема в умовах цифровізації. Актуальність дослідження полягає в ідентифікації кіберзагроз та визначенні основних аспектів захисту від них, що спирається на наукові судження та практичні огляди. **Мета і методи.** Мета статті полягає у дослідженні сутності кіберзахисту брендів та обґрунтуванні механізму його забезпечення. Інтерпретована для розвідки наукова тематика обумовила використання загальнонаукових і спеціальних методів, що дозволили визначити операційні дефініції та побудувати гіпотетичний інструментарій дослідження. Так, для формулювання теоретичних підходів були застосовані методи аналізу, синтезу та індукції. Для оцінювання кіберзагроз і потенційного впливу цифрових інновацій на можливості кіберзахисту було використано метод

сканування горизонту. Зі свого боку, моделювання було використано для створення референтної моделі кіберзахисту готельного бренду. В процесі формування візуального сценарію форсайту кіберзахисту готельних брендів у ракурсі розвитку цифрових технологій було застосовано метод технологічної дорожньої карти, який спирається на апріорні сюжети й точки критичних рішень.

**Результати.** Здійснено опрацювання дефініції «кіберзахист», визначено його основні елементи. Зроблено акцент на цифрових комунікаціях як ключових драйверах системи продажів, що провокують ризики для безпеки готельного бренду. Оцінено параметри готельних брендів, що працюють в Україні, у динаміці. Охарактеризовано джерела підтримки готельних брендів на формальних і неформальних рівнях комунікацій, що забезпечують кібербезпеку готельного бренду. Розглянуто ключові проблеми забезпечення кіберзахисту брендів в Україні, зокрема недостатня увага до управління ризиками, що спричиняє фінансові й репутаційні втрати, а також зупинки бізнес-процесів готелю. Запропоновано напрямки підвищення рівня кіберзахисту на основі використання тактики кіберстійкості, що спирається на носіїв бренду та категорії кіберризиків; а також заходи з управління неформальними каналами комунікації. Перспективами подальших досліджень є оцінювання ефективності управління кіберзахистом суб'єктів готельного бізнесу на тлі зростання кібератак і кіберзагроз в українському цифровому просторі.

**Висновки та обговорення.** Проведене дослідження продемонструвало актуальність наукових опрацювань проблематики кіберзахисту готельного бренду, оскільки дозволяє вивчити та науково обґрунтувати напрями створення стратегічних форпостів, що є необхідною умовою утримання лояльності споживачів та запобігання фінансових і репутаційних втрат для суб'єктів готельного бізнесу, профілактики банкрутства. Використані в дослідженні наукові праці підтверджують важливість захисту бренду у цифровому просторі, що є елементом економічної безпеки готелю.

***Ключові слова:*** кіберзахист, кібербезпека, кіберризики, готельний бренд, цифровий простір, технологічна дорожня карта, сканування горизонту.

## Актуальність проблеми

*Постановка проблеми.* В умовах тотальної цифровізації суб'єкти господарювання є залежними від мультифакторних екзогенних впливів, зокрема у кіберпросторі, що створюють як можливості, так і загрози. Пандемія та війна в Україні сформували нові бачення цифрових відносин, які потребують захисту від дезінформації, кібератак та кіберінцидентів. Готельні бренди сьогодні також залучені в інформаційні війни у супротиві російській руйнівній агресії, переживаючи новий вид кризи. Зважаючи на це, кіберзахист стає однією зі стратегічних цілей економічної безпеки готельного бренду, а актуальність полягає у визначенні його напрямів форсайтингового таймфрейму.

*Стан вивчення проблеми.* У фокусі проблематики цього дослідження перебувають такі аспекти готельного бізнесу, як бренд і кіберзахист, що окреслює відповідне коло наукових джерел. Так, питання щодо формування та управління брендом висвітлені у працях Н. Карачиної (2017), Д. Файвішенко (2020). Щодо політики комунікацій бренду, то окремі питання з інструментарію відображені у працях Н. Овсієнко (2021) та M. Kirnosova (2021). Комунікаційну стратегію бренду у цифровому просторі через точки дотику зі споживачем характеризував Р. Буряк (2019). Практичному огляду аспектів брендингу у сфері готельного бізнесу присвячено дослідження К. Бліщук та І. Козак (2022).

Водночас в умовах глобальної цифровізації під впливом пандемічних локдаунів, що охопили усі сфери життєдіяльності суспільства, наукові дослідження активізувалися навколо питань кібербезпеки та кіберзахисту. Так, C. Guitton (2017), Y. Creado та V. Ramteke (2020) у своїх працях проаналізували на концептуальному і практичному рівнях можливі заходи запобігання кібератакам. Y. Raban та A. Hauptman (Raban & Hauptman, 2018) здійснили форсайт-дослідження для виявлення основних рушійних факторів суттєвої загрози та нових технологій у сфері кібербезпеки. Еволюцію та правові аспекти кібервійни на європейському і міжнародному рівнях розглянули K. Pipyros, L. Mitrou, etc (Pipyros et al., 2016). Практичні аспекти кіберзахисту суб'єктами бізнесу вивчали A. Tuna та Z. Türkmendağ (2022), зокрема питання управління кіберконфліктами та кібервійнами між підприємствами-конкурентами; C. Asbaş та Tuzlukaya (2022) дослідили цілі та методи кібератак, а також розробили бізнес-стратегії їхній протидії; H. S. Chen та J. Fiscus (2018) здійснили оцінку кіберризиків у сфері гостинності тощо. Щодо практичних застосувань у готельному бізнесі з'ясовано, що дослідження мають непрямий характер, зокрема стосуються питань захисту даних (Arcuri et al., 2020; Gwebu & Barrows, 2020; Thomaidis, 2022); управління корпоративними ризиками (Vij, 2019) та окремого формату кіберризиків – сервісної роботизації (G. McCartney & A. McCartney, 2020). Використані в огляді наукові джерела пов'язані схожою метою – обґрунтуванням напрямів кіберзахисту, що для готельних брендів в умовах цифрового середовища виступає тактичним завданням забезпечення конкурентоспроможності.

*Невирішені питання*. Актуальність дослідження полягає в обґрунтуванні положень щодо кіберзахисту готельних брендів, а також ідентифікації кіберризиків, що технологічно еволюціонують у цифровому середовищі.

**Мета і методи досліджень**

*Метою статті* є дослідження сутності кіберзахисту готельних брендів та обґрунтування механізму його забезпечення.

*Методи дослідження*. Дослідження ґрунтується на ідентифікації кіберризиків та формулюванні бізнес-процесів суб'єктів готельного бізнесу щодо захисту власного бренду. Компаративний аналіз поняття «кіберзахист» виявив комплексність напрямів його забезпечення у функціонуванні готельного бренду, що виявляється в процесі цифрових комунікацій зі споживачами, стейкхолдерами та відвідувачами цифрових каналів готелю. Для оцінювання кіберзагроз і потенційного впливу цифрових інновацій на можливості кіберзахисту було використано метод сканування горизонту, що дозволило ідентифікувати та систематизувати ключові кіберризики для готельного бренду. У формуванні практичного контенту забезпечення кіберзахисту готельного бренду було запропоновано референтну модель, опрацьовану за допомогою інструментарію методу моделювання. Цей метод допоміг визначити, яким чином кіберзахист фільтрує систему комунікацій між готельним брендом та комунікатором (клієнтом, відвідувачем цифрової платформи бренду, стейкхолдером). Крім того, в процесі формування візуального сценарію форсайту кіберзахисту готельних брендів у ракурсі розвитку цифрових технологій було застосовано метод технологічної дорожньої карти, який спирається на апріорні сюжети й точки критичних рішень. Щоб оцінити стратегічні

форпости забезпечення кіберзахисту, ми врахували покрокові бізнес-операції, де готельний бренд зазначає ключові точки дотику в комунікаціях із брендом.

*Об'єктом дослідження* визначено процес впровадження та реалізації заходів із кіберзахисту в діяльність готельних брендів.

*Предметом дослідження* є ключові аспекти забезпечення кіберзахисту готельних брендів.

*Наукова новизна* полягає у визначенні напрямів кіберзахисту готельних брендів в Україні, що дозволить забезпечити ефективне управління ризиками та підтримку конкурентоспроможності.

*Інформаційною базою дослідження* є вітчизняні та зарубіжні наукові розробки з кіберзахисту, кібербезпеки, брендингу; онлайн-аналітика та власні спостереження.

**Результати дослідження**

У період пандемічного локдауну цифровий простір розширився, тому зросла кількість точок дотику бренду зі споживачем, а також збільшився обсяг інформації, що надходить із каналів, які власники бренду не контролюють (Буряк, 2019). Тому забезпечення кіберзахисту бренду сьогодні є актуальним питанням і потребує особливої уваги, адже втратити лояльність споживача можна одномоментно внаслідок кібератаки, кіберінциденту, неадекватного посту в соціальних медіа тощо. У цьому ракурсі важливим є опрацювання теоретичного базису та практичних апробацій, що передбачає ідентифікацію понять «готельний бренд» та «кіберзахист», а також розробку моделей управління кіберзахистом бренду.

Розглянемо поняття «бренд» із різних поглядів: у лінгвістичному векторі – це клеймо, спосіб ідентифікації продукції; для маркетологів – сума якостей товару, які роблять кожну окрему купівельну пропозицію унікальною та впізнаваною; для стратегів – засіб управління відносинами між організацією та її цільовою аудиторією (Карачина, 2017). Також проведений нами дефініційний аналіз за науковими джерелами (Карачина, 2017; Файвішенко, 2020; Овсієнко, 2021; Буряк, 2019; Kirnosova, 2021; Бліщук & Козак, 2022) показав відсутність значних дискусійних розбіжностей із його інтерпретації, тому дозволив сформулювати компліментарне визначення бренду як нематеріального активу, що ідентифікує ціннісний образ об'єкта (локації, компанії, продукту тощо) через комунікативний вплив на споживача, формуючи у нього апріорну чи апостеріорну схильність (лояльність).

Зі свого боку, опрацювання правових і наукових положень із кіберзахисту виявило наступні підходи до характеристики терміна:

– сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості й надійності функціонування комунікаційних, технологічних систем (Верховна Рада України, 2017);

– виявлення основних рушійних факторів суттєвої загрози і нових технологій, які, ймовірно, матимуть значний вплив на можливості захисту та атак у сфері кібербезпеки (Raban & Hauptman, 2018);

– механізм захисту комп'ютерної мережі, який включає реагування на дії та захист критичної інфраструктури і забезпечення інформації, а також зосереджу-

ється на запобіганні, виявленні та наданні своєчасного реагування на атаки чи погрози, щоб жодна інфраструктура чи інформація не була підроблена ("Що таке кіберзахист?", 2022);

– сукупність заходів з усунення прогалин у безпеці, забезпечення конфіденційності інформації та захист даних клієнтів (Tuna & Türkmendağ, 2022) тощо.

Контамінація ключових елементів дефініцій «бренд» та «кіберзахист» із зазначених джерел дозволяють трактувати кіберзахист готельного бренду як комплекс заходів і дій, що зосереджуються на запобіганні, виявленні та своєчасному реагуванні на загрози функціонування комунікаційних, технологічних систем, а також протидії атакам інтелектуальної власності, що спричиняють фінансові та репутаційні втрати суб'єкта готельного бізнесу.

У цьому контексті важливо визначити можливі стратегічні напрями кіберзахисту та точки дотику із загрозами готельного бренду.

Загалом стратегія кіберзахисту безпосередньо включає наступні етапи (рис. 1).

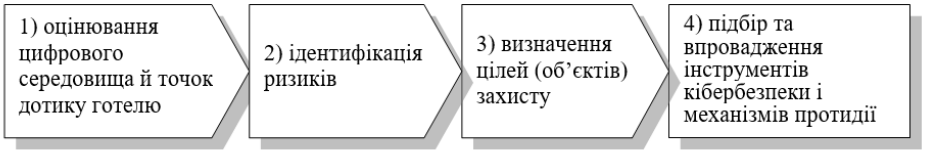


*Рис. 1.* Алгоритм формування стратегії кіберзахисту готелю
*Джерело:* складено за (Creado & Ramteke, 2020; Tuna & Türkmendağ, 2022)

*Pic. 1.* Algorithm of hotel cyber protection strategy formation
*Source:* composed according to (Creado & Ramteke, 2020; Tuna & Türkmendağ, 2022)

Оцінювання кіберзагроз здійснюється через призму цифрових технологій і трендів ринку, які сьогодні демонструють поступове впровадження штучного інтелекту в бізнес-процеси та операції різних сфер діяльності. З цією метою застосуємо метод сканування горизонту, результати якого продемонстровані в табл. 1.

Як бачимо з табл. 1, розвиток інформаційних технологій, що активно почався у 2017 році як поступ четвертої промислової революції та каталізувався коронавірусним локдауном у 2020 році, призвів до пошуку комунікативних ресурсів і технологій: формування IoT, збільшення обсягів даних, поява хмарних і геймінгових технологій, цифрових платформ тощо. Крім того, такі компоненти Індустрії 4.0, як штучний інтелект, доповнена реальність, адитивне виробництво, композитні матеріали, мультиагентні системи, мікросервіси, кібербезпека тощо, у цифровому середовищі масштабували можливості до глобальних охоплень та наблизили суспільство до свідомого використання штучного інтелекту, симбіоз із яким (коботи) створює інноваційний крок до індустрії 5.0, що, за висновками експертів, стартував у 2022 році.

*Табл. 1.* Маркери сканування горизонту викликів кіберпростору для готельних брендів
*Tabl. 1.* Horizon scanning indicators of cyberspace challenges for hotel brands

| **Ключові напрямки** | **Сканування горизонту, 2017–2022 рр. (еволюція: поява та розвиток)** | **Ефект (позитивний – «+», негативний – «-»)** |
|---|---|---|
| товарна інновація (виробництво нового виду продукції/послуг) | поява та комодизація цифрових продуктів: сервісних і безпекових; хмарних і геймінгових продуктів/технологій; доповнена реальність (AR, VR) | ± |
| технологічна інновація (розробка нового методу виробництва/сервісу) | поява штучного інтелекту; коботів (симбіозу роботів та ШІ); дронів; адитивне виробництво, композитні матеріали, мультиагентні системи, мікросервіси | ± |
| ринкова інновація (створення нового ринку товарів/послуг) | формування IoT, ринку цифрових продуктів, кібербезпеки та кіберстрахування; геймінгу | ± |
| маркетингова інновація (освоєння нового джерела поставки ресурсів) | поява Data Science та цифрових платформ для продажу ресурсів, товарів і послуг: байєри в соцмережах, маркетплейси; дистрибуційні платформи | ± |
| управлінська інновація (реорганізація структури управління) | управління командами та проєктами на основі Agile та Lean, онлайн-конференції в Google Meet, Zoom, Teams тощо; інструменти спільної роботи й доступу в Google, OneDrive тощо | ± |

*Джерело:* розроблено авторами за (Заниздра, 2020; "Безпека: головні тренди 2022", б.д.; Mordor Intelligence, 2022)
*Source:* elaborated by authors, according to (Zanizdra, 2020; "Bezpeka: holovni trendy 2022", n.d.; Mordor Intelligence, 2022)

Післяфорсайтний моніторинг дозволяє виокремити наступні тренди цифровізації, які є предметом кіберзахисту готельних брендів (табл. 2).

У діяльності готельних брендів використання ШІ-додатків та опцій є важливим у розвитку комунікацій і гарантування безпеки, зокрема в циклах онлайн-бронювання, фідбеку, застосування ANPR-продуктів для паркінгу, систем на основі розумної відеоаналітики для мінімізації випадків помилкових спрацьовувань та моніторингу проблематичних і безпекових (пожежі, затоплення, задимлення тощо) ситуацій, виникнення конфліктів у приміщеннях загального користування за допомогою аналітики нейромережі тощо.

Слід зазначити, що пандемічна криза, помножена на військову, дестабілізує роботу готельних брендів у різних точках дотику комунікативного процесу ("Як вижити брендові", б.д.):

1) персонал як носій бренду у кризовій ситуації не має цілісної позиції та сценарію щодо реагування й дії, а тому може поширювати дезінформацію і чутки;

*Табл. 2.* Рівні та об'єкти захисту у системі цифрової безпеки готельного бренду
*Tabl. 2.* Levels and objects of protection in digital security system of hotel brand

| **Предмет захисту** | **Рівні захисту** | **Характеристика** |
|---|---|---|
| нові ультратехнологічні рішення на базі штучного інтелекту (ШІ) | *Фізична* (захист майна та цінностей) *безпека* | – нейромережа: розпізнавання загроз пожежної безпеки, контролю роботи елементів критичної інфраструктури будівлі готелю (електро-, водо-, енергопостачання тощо), система доступу до приміщень готелю сторонніх осіб тощо;<br>– система smart-house;<br>– електронні (мобільні) ключі від готельних номерів із функціями засобу платежу в готелі;<br>– системи захисту майна та цінностей споживачів |
| | Комунікативна безпека | – CRM-платформи – системи взаємодії зі споживачами;<br>– налагоджена система геоаналітики, геосервісів та геокарт;<br>– комплексний сервіс зворотного зв'язку і NPS типу Revizion;<br>– клієнтоорієнтована підтримка (коботи, роботи-консьєржі, чатботи, ANPR-продукти, нейромережа) |
| засоби AIoT (поєднання ШІ та інтернету речей) | Безпека системи збуту готельного продукту | – узгоджене функціонування внутрішньої системи управління майном готелю (Internal Property Management System) із мережею дистрибуторів готельних послуг;<br>– налагоджена система комунікації на різних платформах агрегації пропозиції готельних послуг (OTA – онлайн туристичні агенти, IDS – internet дистрибуційні системи, ADS – альтернативні дистрибуційні системи, GDS – глобальні дистрибуційні системи (Amadeus, Sabre, Worldspan, Galileo);<br>захист брендбуку (сайту) готелю |
| хмарні рішення та послуги | Інформаційна безпека | – система захисту внутрішньої конфіденційної інформації щодо поточного фінансового стану, передачі даних комерційного характеру тощо |
| конвергентні системи в організації кіберзахисту систем та інформації | | – системи відеоконтролю;<br>– СКУД;<br>– різного роду сигналізації тощо |
| стабільність та точність передачі даних у режимі 24/7 | | – антивірусні бази захисту даних на внутрішніх серверах;<br>– захист від хакерських атак тощо;<br>– запобігання будь-яким зливам інформації, підвищення рівня безпеки ультрасучасних інформаційних систем тощо |
| Концепція Zero Trust | Інформаційна безпека, захист персональних даних | |

*Продовження табл. 2*

| Предмет захисту | Рівні захисту | Характеристика |
|---|---|---|
| екологізація інновацій та енергоефективні технології | Безпека репутації та іміджу | – використання екологічно безпечних матеріалів та енергоефективних технологій |

*Джерело:* розроблено авторами за ("Безпека: головні тренди 2022", б.д.)
*Source:* elaborated by authors, according to (("Bezpeka: holovni trendy 2022", n.d.)

2) партнери і контрагенти, які не розуміють внутрішніх процесів у готелі, можуть відмовитися від співпраці;

3) медійники і громадськість, які можуть поширювати недостовірні дані, непідкріплені коментарями і фактами;

4) клієнти, комунікацію з якими можна цілком втратити. Тому кіберзахисту потребують інтелектуальні (зокрема, інформаційні) ресурси готельного бренду, які є його власністю та інструментами комунікацій.

З огляду на це, кіберзахист готельного бренду від інформаційного оточення, що може негативно впливати на його імідж і місію, передбачає моніторинг згадок готелю у контенті, що суперечить його політиці, має несприятливий контекст тощо (Kirnosova, 2021), а також відгуків і посилань на рівень сервісу на інших цифрових каналах, зокрема у соціальних мережах. Серед готельних брендів слід відзначити міжнародних готельних операторів, які, згідно з даними річного звіту, є найдорожчими та найсильнішими, а значить, вразливими до репутаційних потрясінь від кібератак (табл. 3).

*Табл. 3.* Рейтинг найсильніших готельних брендів
*Tabl. 3.* Rating scheme of the strongest hotel brands

| Готельний бренд | 2022 | 2021 | зміна | 2020 | зміна |
|---|---|---|---|---|---|
| Taj | 1 | 1 | 0 | new | ↑ |
| Premier Inn | 2 | 2 | 0 | 1 | ↓1 |
| Hilton | 3 | 11 | ↑7 | 7 | ↓4 |
| Hampton Inn | 4 | 6 | ↑2 | 6 | 0 |
| Embassy Suites Hotels | 5 | 20 | ↑15 | 19 | ↓1 |
| Marriot | 6 | 48 | ↑42 | - | - |
| Shangri-La | 7 | 5 | ↓2 | 4 | ↓1 |
| Residence Inn | 8 | 22 | ↑14 | - | - |
| Waldorf Astoria | 9 | 9 | 0 | 2 | ↓7 |
| Wordwide | 10 | 21 | ↑11 | - | - |

*Джерело:* узагальнено авторами за (Brand Finance, 2022)
*Source:* generalised by authors, according to (Brand Finance, 2022)

Як бачимо з табл. 3, у 2022 р. порівняно з попереднім 2021 р. утримали свої позиції готельні бренди Taj (1 місце), Premier Inn (2 місце) та Waldorf Astoria (9 місце). Більшість посилили свої позиції, крім бренду Shangri-La.

Щодо цінності бренду, то його динаміка демонструє наступну рейтингову ситуацію серед міжнародних готельних брендів (рис. 2).

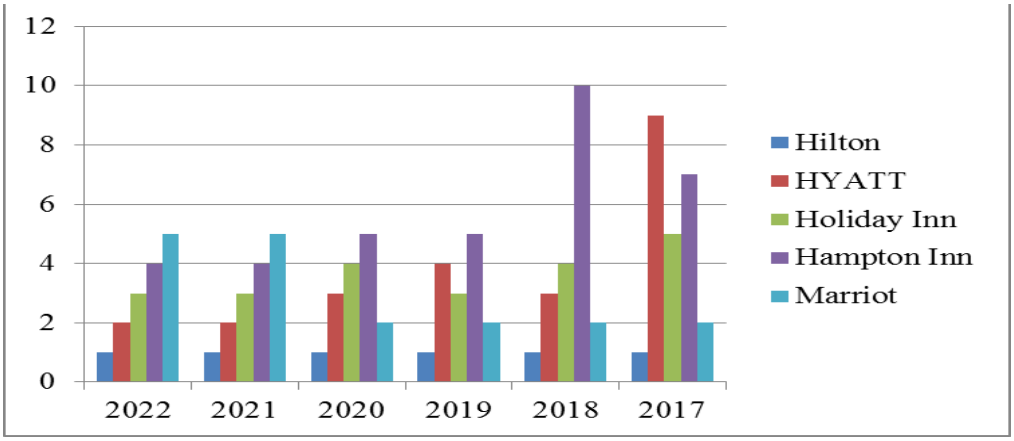


*Рис. 2.* Динамічна карта рейтингу міжнародних готельних брендів, 2017–2022 рр.
*Джерело:* сформовано авторами за (Brand Finance, 2022)

*Pic. 2.* Dynamic rating map of international hotel brands, 2017–2022
*Source:* generated by authors, according to (Brand Finance, 2022)

Аналітика показує, що за 2017–2022 рр. топ-позиції рейтингу практично не змінюються, що свідчить про стабільність готельних операторів на світовому ринку. Серед репрезентованих готельних брендів слід виокремити Hilton та Marriot, включених як у рейтинг найсильніших брендів, так і рейтинг цінності бренду, що представлені на українському ринку брендами Hilton та 11Mirror Design Hotels (під «парасолькою» Marriot). Хоча ковідний період та війна в Україні негативно впливають на їхній розвиток, зокрема зволікання з виходом із ринку країни-агресора Росії (Картер, 2022). Таким чином, вітчизняні суб'єкти готельного бізнесу в реаліях війни з Росією та постійних інформаційних (хакерських) атак стикаються з наступними цифровими ризиками (Бойко та ін., 2022; Мамонова & Позднякова, 2020; Приказюк & Гуменюк, 2020):

– інформаційний спамінг неперевірених та перевірених повідомлень;
– дезорієнтуючі та неправдиві контенти з фейкових месенджерів;
– порушення інформаційної безпеки: ураження вірусами, знищення, модифікація або видалення інформації, фізична крадіжка або втрата обладнання;
– пошкодження програмного забезпечення або комп'ютерів;
– крадіжка або знищення інформації;
– фішинг, вішинг, картинг, фармінг – технології, застосування яких спричиняють крадіжку і використання конфіденційних даних готелю, його клієнтів, партнерів.

Ідентифікація перерахованих ризиків забезпечує підготовку і вироблення сценаріїв протидії та мінімізації втрат від їх настання. Так, для убезпечення репу-

тації готельного бренду потрібно формувати професійну стратегію кіберзахисту, що спиратиметься на протидію загрозам та захист наступних об'єктів (Ліга Закон, 2021): система цифрових комунікацій (сайт, соціальні сторінки, блоги); електронна мережа (системи бронювання та реєстрації); електронна пошта; хмарні сервіси; розрахункові системи; кінцеві точки ІТ-інфраструктури готелю (сервери, ПК, ноутбуки, смартфони тощо).

Отже, управління кіберзахистом готельного бренду буде спрямоване на досягнення стану його захищеності від імовірних репутаційних та фінансових загроз і стресів, що забезпечується постійним моніторингом і контролем над технічними, технологічними та комунікативними бізнес-процесами у кіберсередовищі та відповідальністю за збереження даних самого бренду, його клієнтів, стейкхолдерів. Вищезазначене дозволяє змоделювати основні аспекти забезпечення кіберзахисту готельного бренду (рис. 3).


*Рис. 3.* Референтна модель управління кіберзахистом готельного бренду
*Джерело:* розроблено авторами за (Верховна Рада України, 2017; Arcuri M. et al., 2020; Creado & Ramteke, 2020; Мамонова & Позднякова, 2020; Приказюк & Гуменюк, 2020; Сагірова, 2021; Ліга Закон, 2021; Бойко та ін., 2022; Газізова, 2022)

*Pic. 3.* Referent model of hotel brand cyber protection management
Source: elaborated by authors, according to (Verkhovna Rada of Ukraine, 2017; Arcuri et al., 2020; Creado & Ramteke, 2020; Mamonova & Pozdniakova, 2020; Prykazyuk & Humenyuk, 2020; Sahirova, 2021; Liha Zakon, 2021; Boyko et al., 2022; Hazizova, 2022)

Профілактика ризиків полягає в їхній ідентифікації та категоризації. Так, їх прийнято розділяти на наступні групи: ділові, організаційні та технічні (Kirnosova, 2021). Ділові ризики (або ризики бізнес-процесів) при виникненні знижують фінансові вигоди та вартість бренду, тому безпосередньо пов'язані з комунікаціями готельного бренду у кіберпросторі. Організаційні, зі свого боку, пов'язані із роботою на власному сайті (брендбуці), соціальних сторінках; із хмарними технологіями та моніторингом контенту дистрибуторів, що у кіберпросторі загалом можуть призвести до серйозних збоїв у бізнесі та репутаційних втрат.

Зокрема, варто виділити організаційні питання операційного контексту готелю як користувача та хмарного постачальника. Технічні ризики включають ймовірність впливу шкідливого коду на хмарну платформу, атаки на рівні гіпервізора, витік даних, збої в роботі системи або несанкціоновану передачу тощо. Зокрема, втрата конфіденційності для готельного бренду означатиме ще й репутаційні утрачання, відновити які майже неможливо.

Щодо страхування кіберризику, то страхові відшкодування покривають такі витрати готельного бренду: порушення інформаційної безпеки через ураження вірусами, знищення, модифікація або видалення інформації, фізична крадіжка або втрата обладнання; пошкодження програмного забезпечення або комп'ютерів; крадіжка або знищення інформації. Кіберінциденти спричиняють витрати на юридичний супровід, покриття суми штрафів і стягнень; позовні витрати у зв'язку з відповідальністю щодо злому бази даних конфіденційної інформації. При виникненні ситуацій фітингу та картингу, внаслідок яких відбулися втрати грошових коштів і активів готелю, можливі тактики із профілактики (компетентне управління системами кіберзахисту), страхування та швидкі дії з відновлення репутаційних і фінансових втрат.

У ракурсі розвитку цифрових технологій пропонуємо застосувати такий метод форсайту кіберзахисту готельних брендів, як технологічну дорожню карту, що спирається на апріорні сюжети й точки критичних рішень у кіберпросторі функціонування готельного бренду (табл. 4).

*Табл. 4.* Проєктування технологічної дорожньої карти кіберзахисту готельних брендів

*Tabl. 4.* Projecting a technological road map of hotel brands cyber protection

| **Модуль** | **Сценарії дій / технічні опції** | **Результат** |
|---|---|---|
| Маркетинг | проведення маркетингових досліджень | аналітичні карти форсайту розвитку технологій та розробка цілей кіберзахисту |
| Технології | аналіз існуючих технологій кіберзахисту | оцінка ефективності й доцільності пропозицій (продуктів, послуг) із впровадження кіберзахисту |
| Програми | аналіз стратегій і тактик розвитку бренду в кіберпросторі | стратегія і тактика кіберзахисту готельного бренду |
| Ресурси | аналіз потреб у ресурсах | оцінка витрат ресурсів із забезпечення кіберзахисту та джерел їх покриття |
| Час | аналіз важливості і терміновості реалізації певних заходів із кібербезпеки готельного бренду | календарний план заходів із впровадження, тестування і контролю кіберзахисних дій |

*Продовження табл. 4*

| Модуль | Сценарії дій / технічні опції | Результат |
|---|---|---|
| Ризики | аналіз зовнішнього та внутрішнього кібероточення бренду | план ідентифікації та управління кіберризиками |
| Моніторинг | аналіз імовірностей кіберзагроз, контроль над реакціями на кіберзагрози та оцінка наслідків | контроль над кіберзагрозами, їх проявом та протидіями |

*Джерело:* розроблено авторами за (Артюхов, 2019)
*Source:* elaborated by authors, according to (Artiukhov, 2019)

Наведена дорожня карта демонструє поетапність розробки кіберзахисту у довгостроковій перспективі за рахунок синхронного розвитку технологій, програм, бізнесу і ринку, надає результати (інформацію), що допомагають готельним брендам приймати адекватні рішення щодо інвестицій у кібертехнології у порівнянні з очікуваними кіберризиками. При цьому реалізація заходів із кіберзахисту забезпечується колінеарно до виникнення нових видів кіберзлочинів та атак. Карту розвитку системи забезпечення кіберзахисту представлено на рис. 4.

Слід зазначити, що поєднання зазначених у карті розвитку етапів потребує створення «прошарку», що забезпечить кіберзахист готельного бренду за рахунок створення механізмів протидії (страхування, виведення активів у безпечну цифрову/фінансову зону тощо) та інструментів (антивірусних антихакерських та інших сервісів і платформ захисту).

Таким чином, кіберзахист готельного бренду з використанням пропонованого нами інструментарію його забезпечення створить умови логічного та послідовного управління, зокрема форсайту та розгортання стратегічних, тактичних й оперативних реакцій на загрози кіберсередовища, яке еволюціонує відповідно до появи технічних і технологічних інновацій, симбіотики штучного інтелекту з роботами й людським мозком тощо.

**Висновки та обговорення результатів**

Проведене дослідження із забезпечення кіберзахисту показало актуальність постійного моніторингу загроз для готелів, що можуть бути об'єктами кіберзлочинів. Тому розроблення наукового підходу до кіберзахисту готельних брендів сьогодні є підґрунтям формування технологічних дорожніх карт, що допомагають орієнтуватися в сьогочасних умовах, коли кожен необережний відгук чи пост в інтернеті стає початком кінця для бізнесу.

Операціоналізація теоретичного базису була здійснена на підставі підходів, сформульованих у науковій літературі до визначення термінів «бренд» та «кіберзахист». Так, бренд представлено у дослідженні як нематеріальний актив, що ідентифікує ціннісний образ об'єкта (локації, компанії, продукту тощо) через комунікативний вплив на споживача, формуючи у нього апріорну чи апостеріорну схильність (лояльність). Зі свого боку, кіберзахист інтерпретовано як комплекс заходів і дій, що зосереджуються на запобіганні, виявленні та своєчасному реагуванні на загрози функціонування комунікаційних, технологічних систем, а також протидії атакам інтелектуальної власності, що спричиняють фінансові та репутаційні втрати суб'єкта готельного бізнесу.

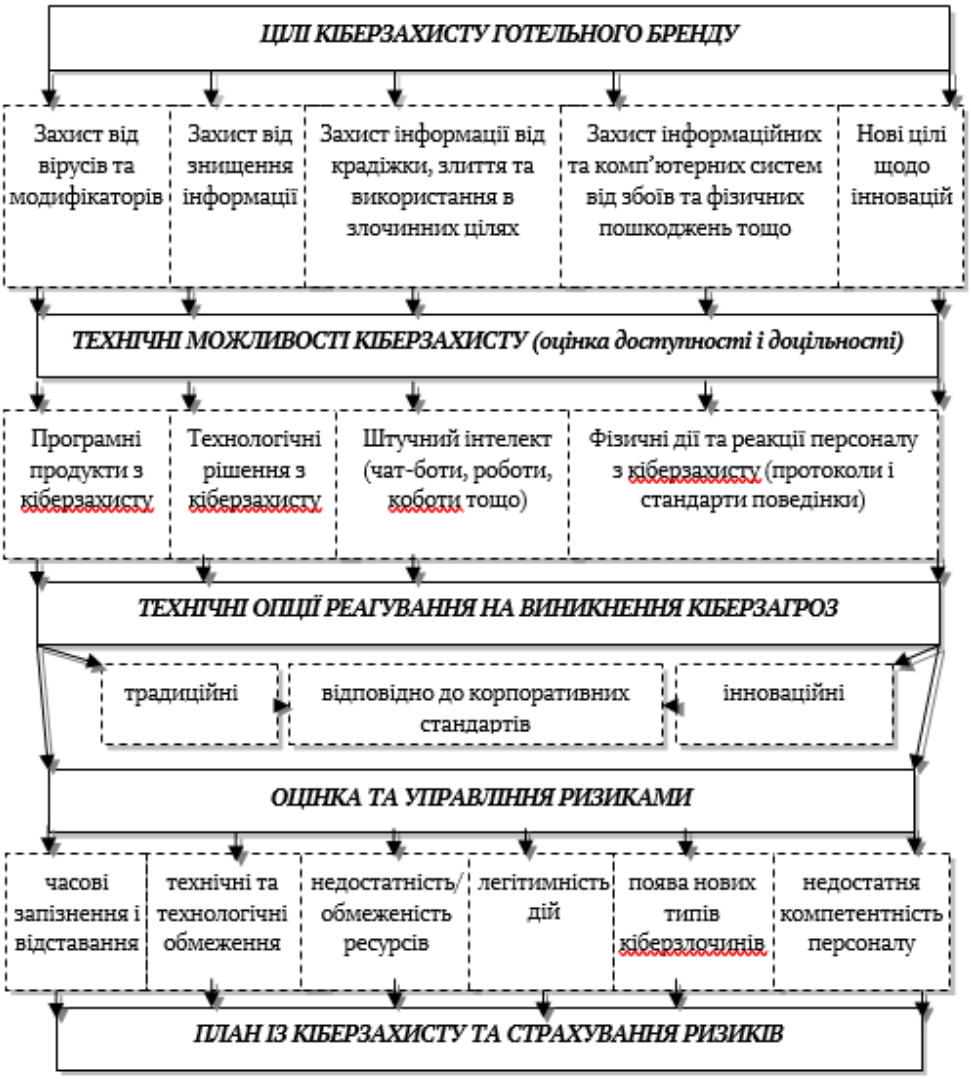


*Рис. 4.* Карта розвитку системи забезпечення кіберзахисту готельного бренду
Джерело: власна розробка

*Pic. 4.* Map of developing the hotel brand cyber protection system
Source: own elaboration

Було визначено стратегічні напрями кіберзахисту та точки дотику із загрозами готельного бренду. На основі цих стратегічних напрямів здійснено оцінювання кіберзагроз через призму цифрових технологій та трендів ринку методом сканування горизонту, результати якого продемонстрували маркери пропозицій щодо управління кіберзахистом готельного бренду: профілактика і страхування ризиків, вироблення реактивних реакцій на загрози, моніторинг та усунення загроз.

Оскільки сильні бренди приваблюють кіберзлочинців, було проаналізовано динаміку рейтингових позицій відомих міжнародних готельних брендів та визначено, що під впливом інформаційної війни вітчизняні готельні бренди є постійними об'єктами кібератак. А через те, що готельний бренд свідомо фактажує унікальний образ якісного і цінного продукту та формує тривалу емоційну прихильність споживача, то у кіберпросторі кіберзахист буде спрямований саме на захист і збереження цих цінностей. Крім того, пандемічна криза і війна в Україні негативно відобразились на фінансовій стабільності готелів, що спричинило потребу в економії, зокрема на використанні консалтингових та аутсорсингових послуг із кіберзахисту, а також утриманні відповідного компетентного персоналу.

Таким чином, було аргументовано, що заходи з управління кіберзахистом готельного бренду спрямовуються на досягнення стану його захищеності від імовірних репутаційних і фінансових загроз та стресів, що забезпечується постійним моніторингом і контролем над технічними, технологічними та комунікативними бізнес-процесами у кіберсередовищі та відповідальністю за збереження даних самого бренду, його клієнтів, стейкхолдерів.

Отже, проблематика кіберзахисту досить широка, що потребує поглиблених опрацювань зазначених нами положень, які доповняться фактажем ефективних практик після закінчення окупаційної війни Росії та спрямовані на перспективу наших наукових досліджень.

## СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

Артюхов, А. Є. (2019). Дорожня карта розвитку систем забезпечення якості освіти у ВНЗ: освітній та соціально-економічний аспекти. *Причорноморські економічні студії, 37, 243–247*. http://bses.in.ua/journals/2019/37_2019/48.pdf

*Безпека: головні тренди 2022*. (б.д.). SmartEl. Взято 15 вересня, 2022 з https://smartel.ua/ua/articles/bezopasnost-glavnye-trendy-2022/

Бліщук, К. М., & Козак, І. І. (2021). Брендинг у сфері готельного бізнесу. *Ефективність державного управління*, *3–4*(68–69), 22–32. https://doi.org/10.36930/506802

Бойко, М., Бовш, Л., & Охріменко, А. (2022). Кризостійкість туристичного бізнесу в умовах воєнного стану. *Товари і ринки, 2*(42), 31–47.

Буряк, Р. В. (2019, 19 березня). Комунікаційна стратегія бренду в цифровому суспільстві. В *Журналістика та реклама: вектори взаємодії*, Тези доповідей Міжнародної науково-практичної конференції (с. 71–74). Київський національний торговельно-економічний університет. http://dx.doi.org/10.31617/k.knute.2019-03-19.24

Верховна Рада України. (2017, 5 жовтня). *Про основні засади забезпечення кібербезпеки України* (Закон № 2163-VIII). https://zakon.rada.gov.ua/laws/show/2163-19#Text

Газізова, Ю. (2022). Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. *Юрист & Закон, 12* (646). https://uz.ligazakon.ua/ua/magazine_article/EA013606

Заниздра, М. (2020). Методы и практика применения экологического форсайта: аналитический обзор. *Економіка промисловості, 2*(90), 93–115. https://doi.org/10.15407/econindustry2020.02.093

Карачина, Н. П. (2017, 15–24 березня). Етимологія та розвиток трактування економічної категорії «бренд». В *Матеріали XLVI науково-технічної конференції підрозділів Вінницького національного технічного університету* (с. 2551–2554). Вінницький національний технічний університет. https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2017/paper/view%20File/3025/2228

Картер, С. (2022, 1 червня). *Marriott і Hilton обмірковують вихід з росії*. UNN. https://www.unn.com.ua/uk/news/1979427-marriott-i-hilton-obmirkovuyut-vikhid-z-rosiyi

Ліга Закон. (2021, 21 грудня). *Бізнес під загрозою кібератаки. Як захистити компанію?* https://biz.ligazakon.net/news/208297_bznes-pd-zagrozoyu-kberataki-yak-zakhistiti-kompanyu

Мамонова, Г., & Позднякова, Л. (2020, 4 грудня). Особливості страхування кібер-ризиків. В *Міждисциплінарні наукові дослідження: особливості та тенденції*, Матеріали Міжнародної наукової конференції (Т. 2, с. 91–93). Міжнародний центр наукових досліджень. https://doi.org/10.36074/04.12.2020.v2.12

Овсієнко, Н. В. (2021). Оптимізація інструментарію маркетингової політики комунікацій діяльності бренду. *Економіка та суспільство, 24*. https://doi.org/10.32782/2524-0072/2021-24-47

Приказюк, Н. В., & Гуменюк, Л. С. (2020). Кібер-страхування як важливий інструмент захисту підприємств в умовах цифровізації економіки. *Ефективна економіка, 4*. https://doi.org/10.32702/2307-2105-2020.4.6

Сагірова, А. (2021). Забезпечення економічної безпеки в готельному бізнесі за допомогою інновацій. *Приазовський економічний вісник*, *1*(24), 104–108. https://doi.org/10.32840/2522-4263/2021-1-17

Файвішенко, Д. (2020, 1 травня). Бренд-стратегія: інструменти планування. В *Наукове забезпечення технологічного прогресу XXI сторіччя*, Матеріали Міжнародної наукової конференції (Т. 1, с. 20–21). Міжнародний центр наукових досліджень. https://doi.org/10.36074/01.05.2020.v1.03

*Що таке кіберзахист? – визначення з техопедії*. (2022). Theastrologypage. https://uk.theastrologypage.com/cyber-defense

*Як вижити брендові у кризовій ситуації, або що робити, якщо медіа офіційно «поховали» компанію*. (б.д.). Executives. Взято 07 березня, 2022 з https://executives.com.ua/yak-vyzhyty-brendovi-u-kryzovii-sytuatsii/

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290. https://doi.org/10.1108/JHTT-05-2019-0080

Asbaş, C., & Tuzlukaya, S. (2022). Cyberattack and Cyberwarfare Strategies for Businesses. In F. Özsungur (Ed.), *Conflict Management in Digital Business* (pp. 303–328). Emerald. https://doi.org/10.1108/978-1-80262-773-220221027

Brand Finance. (2022). *Hotels 50 2022: The annual report on the most valuable and strongest hotel brands*. https://brandirectory.com/download-report/brand-finance-hotels-50-2022-preview.pdf

Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology*, *9*(2), 223–234. https://doi.org/10.1108/JHTT-07-2017-0044

Creado, Y., & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. *Journal of Financial Crime*, *27*(3), 771–780. https://doi.org/10.1108/JFC-01-2020-0008

Guitton, C. (2017, June 19–20). Foiling cyber attacks. In *2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1–7). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/cybersecpods.2017.8074853

Gwebu, K., & Barrows, C. W. (2020). Data breaches in hospitality: is the industry different? *Journal of Hospitality and Tourism Technology*, *11*(3), 511–527. https://doi.org/10.1108/JHTT-11-2019-0138

Kirnosova, M. (2021). Authenticity of brands in the marketing commodity policy of the enterprise. *VUZF Review*, *6*(3), 78–89. https://doi.org/10.38188/2534-9228.21.3.09

McCartney, G., & McCartney, A. (2020). Rise of the machines: towards a conceptual service-robot research framework for the hospitality and tourism industry. *International Journal*

*of Contemporary Hospitality Management*, *32*(12), 3835–3851. https://doi.org/10.1108/IJCHM-05-2020-0450

Mordor Intelligence. (2022, June). *Industry 4.0 Market – Growth, Trends, and Forecasts (2020 – 2025)*. ASDreports. https://www.asdreports.com/market-research-report-538241/industry-market-growth-trends-forecasts

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare. *Information and Computer Security*, *24*(1), 38–52. https://doi.org/10.1108/ICS-12-2014-0081

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight*, *20*(4), 353–363. https://doi.org/10.1108/FS-02-2018-0020

Thomaidis, A. (2022). Data Breaches in Hotel Sector According to General Data Protection Regulation (EU 2016/679). In M. Valeri (Ed.), *Tourism Risk* (pp. 129–140). Emerald. https://doi.org/10.1108/978-1-80117-708-520221009

Tuna, A. A., & Türkmendağ, Z. (2022). Cyber Business Management. In F. Özsungur (Ed.), *Conflict Management in Digital Business* (pp. 281–301). Emerald. https://doi.org/10.1108/978-1-80262-773-220221026

Vij, M. (2019). The emerging importance of risk management and enterprise risk management strategies in the Indian hospitality industry: Senior managements' perspective. *Worldwide Hospitality and Tourism Themes*, *11*(4), 392–403. https://doi.org/10.1108/WHATT-04-2019-0023

## REFERENCES

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290. https://doi.org/10.1108/JHTT-05-2019-0080 [in English].

Artiukhov, A. Ye. (2019). Dorozhnia karta rozvytku system zabezpechennia yakosti osvity u VNZ: osvitnii ta sotsialno-ekonomichnyi aspekty [Roadmap for the development of quality assurance systems in higher education institutions: educational and socio-economic aspects]. *Black sea economic studies, 37*, 243–247. http://bses.in.ua/journals/2019/37_2019/48.pdf [in Ukrainian].

Asbaş, C., & Tuzlukaya, S. (2022). Cyberattack and Cyberwarfare Strategies for Businesses. In F. Özsungur (Ed.), *Conflict Management in Digital Business* (pp. 303–328). Emerald. https://doi.org/10.1108/978-1-80262-773-220221027 [in English].

*Bezpeka: holovni trendy 2022* [Security: the main trends of 2022]. (n.d.). SmartEl. Retrieved September 15, 2022, from https://smartel.ua/ua/articles/bezopasnost-glavnye-trendy-2022/ [in Ukrainian].

Blishchuk, K. M., & Kozak, I. I. (2021). Brendynh u sferi hotelnoho biznesu [Branding in the field of hotel business]. *Efficiency of public administration. 3–4*(68–69), 22–32. https://doi.org/10.36930/506802 [in Ukrainian].

Boiko, M., Bovsh, L., & Okhrimenko, A. (2022). Kryzostiikist turystychnoho biznesu v umovakh voiennoho stanu [Crisis resilience of the tourism business in martial law]. *Commodities and markets, 2*(42), 31–47. https://doi.org/10.31617/2.2022(42)03 [in Ukrainian].

Brand Finance. (2022). *Hotels 50 2022: The annual report on the most valuable and strongest hotel brands*. https://brandirectory.com/download-report/brand-finance-hotels-50-2022-preview.pdf [in English].

Buriak, R. V. (2019, March 19). Komunikatsiina stratehiia brendu v tsyfrovomu suspilstvi [Brand communication strategy in the digital society]. In *Zhurnalistyka ta reklama: vektory vzaiemodii* [Journalism and advertising: vectors of interaction], Abstract of papers of the

International Scientific and Practical Conference (pp. 71–74). Kyiv National University of Trade and Economics. http://dx.doi.org/10.31617/k.knute.2019-03-19.24 [in Ukrainian].

Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology*, *9*(2), 223–234. https://doi.org/10.1108/JHTT-07-2017-0044 [in English].

Creado, Y., & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. *Journal of Financial Crime*, *27*(3), 771–780. https://doi.org/10.1108/JFC-01-2020-0008 [in English].

Faivishenko, D. (2020, May 1). Brend-stratehiia: instrumenty planuvannia [Brand strategy: planning tools]. In *Naukove zabezpechennia tekhnolohichnoho prohresu XXI storichchia* [Scientific support of technological progress of the XXI century], Proceedings of the International Scientific Conference (Vol. 1, pp. 20–21). Mizhnarodnyi tsentr naukovykh doslidzhen. https://doi.org/10.36074/01.05.2020.v1.03 [in Ukrainian].

Guitton, C. (2017, June 19–20). Foiling cyber attacks. In *2017 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1–7). Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/cybersecpods.2017.8074853 [in English].

Gwebu, K., & Barrows, C. W. (2020). Data breaches in hospitality: is the industry different? *Journal of Hospitality and Tourism Technology*, *11*(3), 511–527. https://doi.org/10.1108/JHTT-11-2019-0138 [in English].

Hazizova, Yu. (2022). Kiberzlochynnist v Ukraini. Era tsyfrovykh tekhnolohii – era novykh zlochyniv [Cybercrime in Ukraine. The era of digital technologies is the era of new crimes]. *Yuryst & Zakon, 12* (646). https://uz.ligazakon.ua/ua/magazine_article/EA013606 [in Ukrainian].

Karachyna, N. P. (2017, March 15–24). Etymolohiia ta rozvytok traktuvannia ekonomichnoi katehorii "brend" [Etymology and development of interpretation of the economic category "brand"]. In *Materialy XLVI naukovo-tekhnichnoi konferentsii pidrozdiliv Vinnytskoho natsionalnoho tekhnichnoho universytetu* [Proceedings of the XLVI scientific and technical conference of subdivisions of the Vinnytsia National Technical University] (pp. 2551–2554). Vinnytsia National Technical University. https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2017/paper/view%20File/3025/2228 [in Ukrainian].

Karter, S. (2022, June 1). *Marriott i Hilton obmirkovuiut vykhid z rosii* [Marriott and Hilton are considering exiting russia]. UNN. https://www.unn.com.ua/uk/news/1979427-marriott-i-hilton-obmirkovuyut-vikhid-z-rosiyi [in Ukrainian].

Kirnosova, M. (2021). Authenticity of brands in the marketing commodity policy of the enterprise. *VUZF Review*, *6*(3), 78–89. https://doi.org/10.38188/2534-9228.21.3.09 [in English].

Liha Zakon. (2021, December 21). *Biznes pid zahrozoiu kiberataky. Yak zakhystyty kompaniiu?* [Business is at risk of a cyber attack. How to protect the company?]. https://biz.ligazakon.net/news/208297_bznes-pd-zagrozoyu-kberataki-yak-zakhistiti-kompanyu [in Ukrainian].

Mamonova, H., & Pozdniakova, L. (2020, December 4). Osoblyvosti strakhuvannia kiber-ryzykiv [Features of cyber risk insurance]. In *Mizhdystsyplinarni naukovi doslidzhennia: osoblyvosti ta tendentsii* [Interdisciplinary scientific research: features and trends], Proceedings of the International Scientific Conference (Vol. 2, pp. 91–93). Mizhnarodnyi tsentr naukovykh doslidzhen. https://doi.org/10.36074/04.12.2020.v2.12 [in Ukrainian].

McCartney, G., & McCartney, A. (2020). Rise of the machines: towards a conceptual service-robot research framework for the hospitality and tourism industry. *International Journal of Contemporary Hospitality Management*, *32*(12), 3835–3851. https://doi.org/10.1108/IJCHM-05-2020-0450 [in English].

Mordor Intelligence. (2022, June). *Industry 4.0 Market – Growth, Trends, and Forecasts (2020 – 2025)*. ASDreports. https://www.asdreports.com/market-research-report-538241/industry-market-growth-trends-forecasts [in English].

Ovsiienko, N. V. (2021). Optymizatsiia instrumentariiu marketynhovoi polityky komunikatsii diialnosti brendu [Optimization of marketing policy in brand communication activities]. *Economy and Society, 24*. https://doi.org/10.32782/2524-0072/2021-24-47 [in Ukrainian].

Pipyros, K., Mitrou, L., Gritzalis, D., & Apostolopoulos, T. (2016). Cyberoperations and international humanitarian law: A review of obstacles in applying international law rules in cyber warfare. *Information and Computer Security*, *24*(1), 38–52. https://doi.org/10.1108/ICS-12-2014-0081 [in English].

Prykaziuk, N., & Gumenyuk, L. (2020). Kiber-strakhuvannia yak vazhlyvyi instrument zakhystu pidpryiemstv v umovakh tsyfrovizatsii ekonomiky [Cyber-insurance as an important tool of enterprise protection in the digitization economy]. *Efektyvna ekonomika, 4*. https://doi.org/10.32702/2307-2105-2020.4.6 [in Ukrainian].

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *Foresight*, *20*(4), 353–363. https://doi.org/10.1108/FS-02-2018-0020 [in English].

Sahirova, A. S. (2021). Zabezpechennia ekonomichnoi bezpeky v hotelnomu biznesi za dopomohoiu innovatsii [Ensuring economic security in the hotel business with the help of innovation]. *Pryazovskyi Economic Herald, 1*(24), 104–108. https://doi.org/10.32840/2522-4263/2021-1-17 [in Ukrainian].

*Shcho take kiberzakhyst? – vyznachennia z tekhopedii* [What is cyber security? – definition from technical education]. (2022). Theastrologypage. https://uk.theastrologypage.com/cyber-defense [in Ukrainian].

Thomaidis, A. (2022). Data Breaches in Hotel Sector According to General Data Protection Regulation (EU 2016/679). In M. Valeri (Ed.), *Tourism Risk* (pp. 129–140). Emerald. https://doi.org/10.1108/978-1-80117-708-520221009 [in English].

Tuna, A. A., & Türkmendağ, Z. (2022). Cyber Business Management. In F. Özsungur (Ed.), *Conflict Management in Digital Business* (pp. 281–301). Emerald. https://doi.org/10.1108/978-1-80262-773-220221026 [in English].

*Yak vyzhyty brendovi u kryzovii sytuatsii, abo shcho robyty, yakshcho media ofitsiino "pokhovaly" kompaniiu* [How to survive a brand in a crisis situation, or what to do if the media officially "buried" the company]. (n.d.). Executives. Retrieved March 7, 2022, from https://executives.com.ua/yak-vyzhyty-brendovi-u-kryzovii-sytuatsii/ [in Ukrainian].

Verkhovna Rada of Ukraine. (2017, October 5). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy* [On the Basic Principles of Cybersecurity in Ukraine] (Law № 2163-VIII). https://zakon.rada.gov.ua/laws/show/2163-19#Text [in Ukrainian].

Vij, M. (2019). The emerging importance of risk management and enterprise risk management strategies in the Indian hospitality industry: Senior managements' perspective. *Worldwide Hospitality and Tourism Themes*, *11*(4), 392–403. https://doi.org/10.1108/WHATT-04-2019-0023 [in English].

Zanizdra, M. Yu. (2020). Metody i praktika primeneniya ekologicheskogo forsaita: analiticheskii obzor [Methods and practice of applying environmental foresight: analytical review]. *Economy of Industry, 2*(90), 93–115. https://doi.org/10.15407/econindustry2020.02.093 [in Russian].

Стаття надійшла до редакції 18.09.2022 р.

UDC 640.4:659.126]:004.946.5.056

***Iryna Verezomska,***
*PhD in Economics,*
*Kyiv National University of Culture and Arts,*
*Kyiv, Ukraine,*
*verez_kult@ukr.net*
*https://orcid.org/0000-0002-3289-3734*

***Liudmyla Bovsh,***
*PhD in Economics,*
*State University of Trade and Economics,*
*Kyiv, Ukraine,*
*lbovsh@ukr.net*
*https://orcid.org/0000-0001-6044-3004*

***Kseniia Prykhod`ko,***
*Lecturer,*
*Kyiv National University of Culture and Arts,*
*Kyiv,Ukraine,*
*prykhodko11@ukr.net*
*https://orcid.org/0000-0002-7347-3226*

***Khrystyna Baklan***
*Graduate Student for Master's degree,*
*Kyiv National University of Culture and Arts,*
*Kyiv, Ukraine,*
*gajtynka@ukr.net*
*https://orcid.org/0000-0002-7574-5870*

## CYBER PROTECTION OF HOTEL BRANDS

**Topicality**. The hotel industry suffered significant financial shifts during pandemic, which have been exacerbated by the martial law in Ukraine. The problem of protecting intangible assets has become relevant, in particular, in conditions that some blighty hotels have Russian beneficiaries, and certain international brands have remained their activity in Russia, which unleashed a full-scale war in Ukraine. In addition to physical destruction, hotels have also become the subject of information war and cybercrimes. Therefore, the issue of brands cyber protection has become an important component of the development strategy, over and above, in digitalisation sphere. The topicality of this research lies in cyber threats identification, as well as determination of the main aspects of protection against them. All this mentioned above is based on scientific positions and practical reviews. **The aim of the study and its methods.** The aim of the article is to research the essence of brands cyber protection, and found the mechanism of its provision. Interpreted for the research, the scientific topic has determined the use of general scientific and special methods, which made it possible to define operational definitions, and build a hypothetical study apparatus. Thus, the methods of analysis, synthesis and induction have beed used in order to formulate theoretical approaches. A horizon scanning method has been applied to assess cyber threats and the potential impact of digital innovations on cyber defence capabilities. In turn, modelling has been used for creating a hotel brand cyber defence referent model. In the process of forming a visual scenario of foresight of hotel brands cyber protection in the aspect of digital technologies development, the technological road map method has been applied. It is based on apriori plots and points of critical decisions.

**Results.** The definition of "cyber protection" has been worked out, its main elements have been determined. The emphasis has been placed on digital communications as key drivers of the

sales system, which provoke risks for the hotel brand security. In dynamics, the parameters of hotel brands operating in Ukraine have been evaluated. The sources of support for hotel brands at formal and informal levels of communications, which ensure the hotel brand cyber security, have been characterised. The key problems of ensuring brands cyber protection in Ukraine have been considered. In particular, insufficient attention to risk management, which causes financial and reputational losses, as well as stoppages of hotel business processes, has been highlighted. Directions for increasing the level of cyber protection based on the use of cyber resilience tactics, oriented on brand carriers and cyber risk categories, have been offered, as well as measures in management of informal communication channels. Prospects for further research are the effectiveness evaluation of cyber protection management of hotel business entities on the background of the growth of cyber-attacks and cyber threats in Ukrainian digital space.

**Conclusions and discussion.** The conducted research demonstrates the relevance of scientific studies of the issue of hotel brand cyber protection, as it allows to study and scientifically substantiate the directions of creating strategic outposts, which is a necessary condition for maintaining consumer loyalty, and preventing financial and reputational losses for hotel business entities, additionally, avoiding bankruptcy. Used in this research, scientific works confirm the importance of brand protection in the digital space, which is an element of hotel economic security.

***Keywords****:* cyber protection, cyber security, cyber risks, hotel brand, digital space, technological road map, horizon scanning.