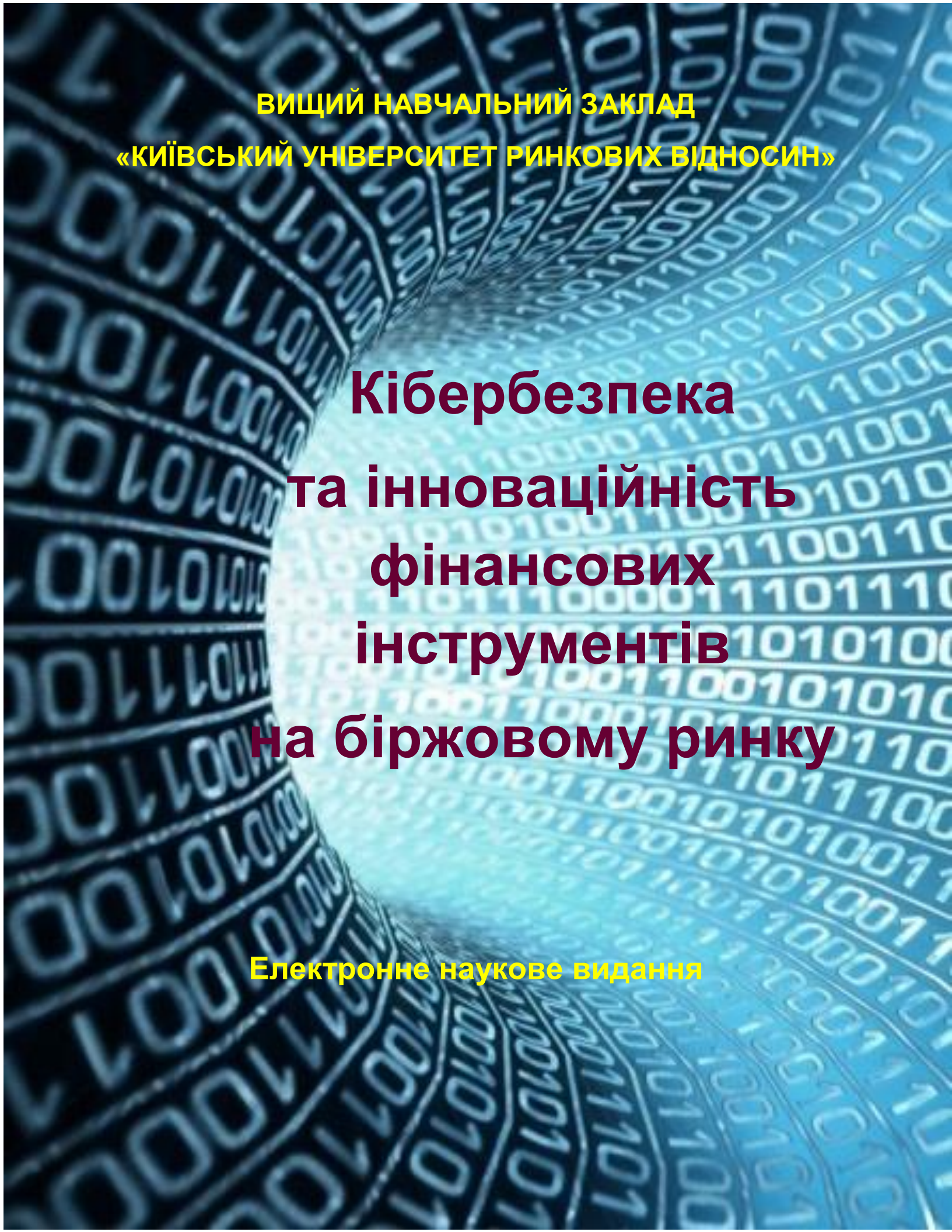
ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«КИЇВСЬКИЙ УНІВЕРСИТЕТ РИНКОВИХ ВІДНОСИН»



Кібербезпека та інноваційність фінансових інструментів на біржовому ринку

Електронне наукове видання

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«КИЇВСЬКИЙ УНІВЕРСИТЕТ РИНКОВИХ ВІДНОСИН»

«Кібербезпека та інноваційність фінансових інструментів на біржовому ринку»

Матеріали круглого столу
(30.11.2023 року)

Електронне наукове видання

Київ

2023

УДК 336:76.02:[004.056+005.591.6

К 46

Рекомендовано до друку рішенням Навчально-методичної ради ВНЗ «Київський університет ринкових відносин», (протокол № 3 від 29.12.2023 р.)

Кібербезпека та інноваційність фінансових інструментів на біржовому ринку: матеріали круглого столу (м. Київ, 30 листопада 2023 р.): електрон. наук. вид. / За наук. ред. О. В. Безпаленко. Київ: ВНЗ «Київський університет ринкових відносин», 2023. 77 с.

Розвиток нових технологій на фінансовому ринку є значним прогресивним кроком, і водночас загрозою у фінансово-економічному просторі. Збалансоване поєднання запровадження нових інноваційних фінансових продуктів та створення надійної системи протидії кіберзлочинності стане важливим стратегічним напрямком у вдосконаленні та активізації функціонуючого біржового ринку в епоху технологічних процесів. В збірнику представлені наукові узагальнення результатів досліджень щодо основних тенденцій та особливостей впровадження фінансових інструментів та захисту від кіберзагроз в Україні.

Для широкого кола науковців, викладачів, аспірантів, студентів і фахівців у сфері економіки і фінансів.

УДК 336:76.02:[004.056+005.591.6

Вищий навчальний заклад
«Київський університет ринкових відносин», 2023

ЗМІСТ

УДК 339.543.642.6
ФОСТОЛОВИЧ Валентина Анатоліївна
доктор економічних наук, доцент кафедри економіки, менеджменту, маркетингу та готельно-ресторанної справи
Житомирського державного університету імені Івана Франка
ORCID: https://orcid.org/0000-0001-5359-7996
ГРИШКОВЕЦЬ Сніжана Анатоліївна
магістр 1-го року навчання
Житомирського державного університету імені Івана Франка
ORCID: https://orcid.org/0009-0001-6323-7828

КІБЕРБЕЗПЕКА ТА УПРАВЛІННЯ ПЕРСОНАЛОМ У ЗАКЛАДІ ГОТЕЛЬНО-РЕСТОРАННОГО БІЗНЕСУ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

У умовах цифрових трансформацій кібербезпека стала одним із найважливіших аспектів у системі управління закладом сфери гостинності та особливо, у частині управління персоналом. Цифрові можливості стали настільки розвинутими, що головна інформаційна база даних підприємств знаходяться в електронному вигляді. Це робить підприємства більш вразливими до кібератак, оскільки вони можуть призвести до: повного або часткового витоку інформації, фінансових втрат, порушення бізнес-процесів, інших негативних наслідків.

Важливим ресурсом захисту підприємств готельно-ресторанного бізнесу від кібератак є ефективне управління персоналом. Людський ресурс (персонал) компанії слугує одним із найважливіших активів компанії. Виважені дії працівників підприємства можуть сприяти запобіганню або мінімізувати наслідки кібератак.

Автоматизація виробничих процесів в готельно-ресторанному бізнесі сприяє їх конкурентоспроможності та економічній безпеці [2], проте, одночасно виступає об’єктом кіберзлочинів.

У своїй діяльності підприємства сфери гостинності використовують інтернет-ресурси та цифрові технології у процесах: бронювання, управління номерним

фондом, системі продажів, маркетингових технологіях, системі обліку і контролю, у системі обслуговування замовлень, у процесі доставки та інше [1].

Результати кібератак мають руйнівні наслідки на діяльність самого підприємства та його економічну безпеку. Вони можуть призвести до фінансових втрат, порушення конфіденційності інформації про клієнтів, і, навіть, до банкрутства бізнесу в будь-який момент, в той час як цього ніхто не очікує.

Підприємства готельно-ресторанного бізнесу з метою захисту від втручань кіберзлочинців та хакерських атак повинні розробити та впровадити ряд заходів у частині:

1. технічних заходів,

2. організаційних заходів;

3. правових заходів.

Нами схематично представлено систему технічних заходів, які підприємство повинно розробити та впровадити у діяльність з метою захисту інформації та власного бізнесу від кібератак (рис. 1).

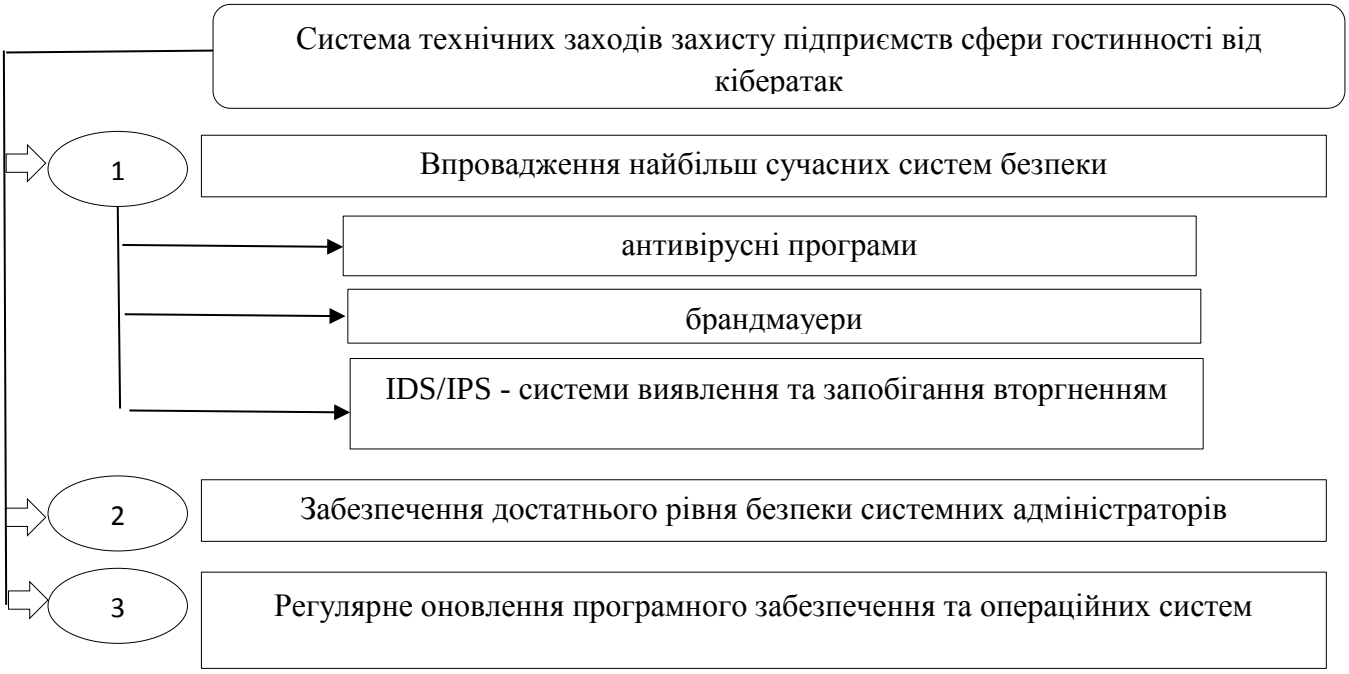


Рис. 1. Система технічних заходів захисту підприємств сфери гостинності від кібератак

Джерело: Сформовано автором

Керівництво підприємств формує та впроваджувати комплекс заходів для забезпечення кібербезпеки, які спрямовані на захист інформаційних систем та мереж від кібератак.

Важливим інструментом є впровадження антивірусні програми, брандмауерів та систем виявлення та запобігання вторгненням (IDS/IPS).

Варто звернути належну увагу також і на забезпечення достатнього рівня підготовки системних адміністраторів у сфері цифрової безпеки.

Проводячи регулярне оновлення програмного забезпечення та операційних систем із встановленням паролів високого рівня захисту підприємство може себе убезпечити від вторгнення у систему кіберзлочинців.

Не менш важливими є організаційні та правові заходи захисту від зовнішніх непередбачених втручань у інформаційну систему та базу даних підприємства. Організаційні заходи, спрямовані на підвищення обізнаності персоналу про кібербезпеку та формування культури кібербезпеки у компанії.

Інструментом формування ефективної системи захисту від кіберзлочинців є:

1) розробка і впровадження політики кібербезпеки;

2) проведення навчальних заходів для персоналу з питань кібербезпеки;

3) запровадження системи контролю за дотриманням політики кібербезпеки.

Застосовуючи правові заходи підприємства сфери гостинності при формуванні баз даних клієнтів повинні забезпечити належний рівень захисту персональних даних. Одним із засобів убезпечення від економічних втрат при кібератаках є придбання страхового полісу від кібератак.

Система управління персоналом несе вагомий вклад у формування інформаційної безпеки підприємства завдяки: розробці і впровадженню політики кібербезпеки; проведенню навчальних заходів для персоналу; запровадженню системи контролю за дотриманням політики кібербезпеки; застосуванню комплексного підходу, в якому управління персоналом відіграє важливу роль.

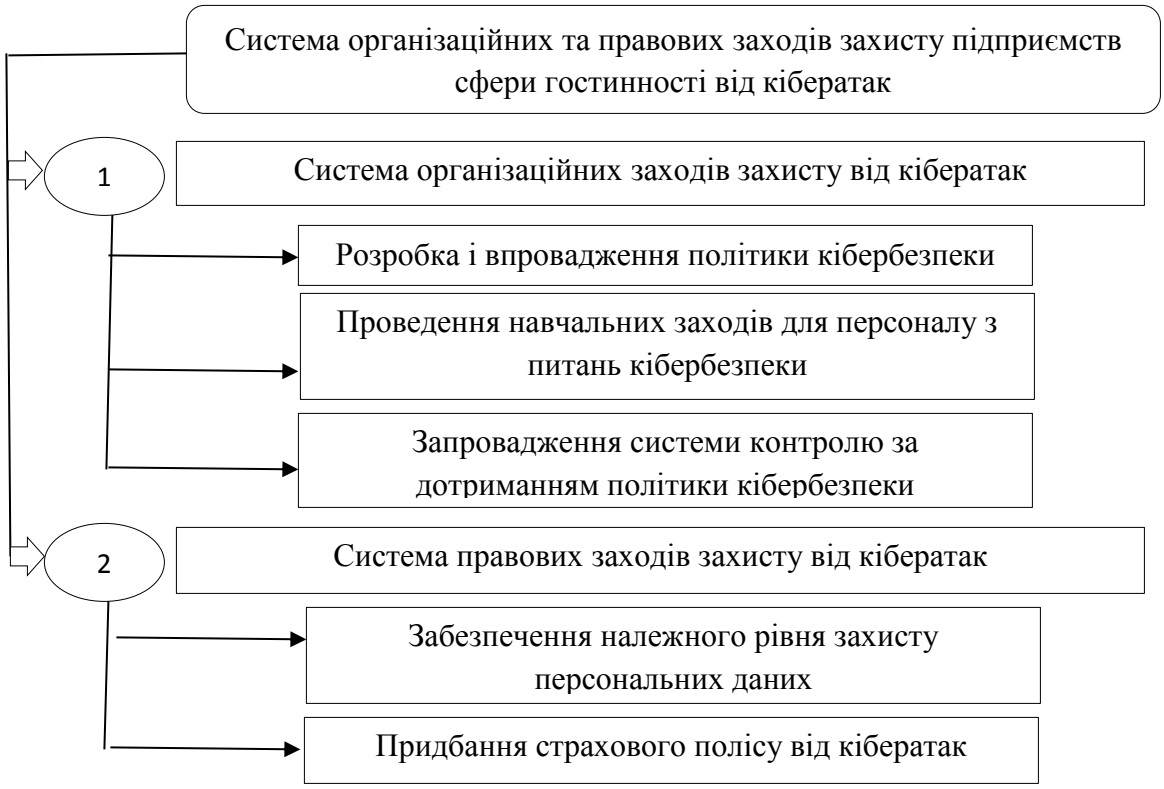


Рис. 2. Система організаційних та правових заходів захисту підприємств сфери гостинності від кібератак

Джерело: Сформовано автором

Розробка та інтегрування політики кібербезпеки. Політика кібербезпеки на підприємствах сфери гостинності визначає:

- розробку основних принципів та правил кібербезпеки в компанії;
- встановлення відповідальності за їх дотримання;

Важливим є те, що у розробці політики кібербезпеки підприємства повинні брати участь працівники відділу управління персоналом.

Часто можливість кіберзлочинів обумовлена необізнаністю працівників підприємства в даному питанні. З метою уникнення даної проблеми слід проводити навчальні заходи для персоналу. Персонал повинен бути обізнаний про основні загрози кібербезпеки та про те, як їх уникнути.

Необхідним інструментом уникнення загроз від кіберзлочинців є запровадження ефективної системи контролю за дотриманням основних

принципів і правил політики кібербезпеки. На підприємстві повинні бути чітко обумовлені:

- правила використання електронної пошти;
- правила користування соціальними мережами;
- правила користування різними цифровими технологіями.

Система контролю повинна здійснювати регулярний моніторинг дотримання співробітниками підприємства політики кібербезпеки. Працівники відділу управління персоналом повинні брати участь в розробці й впровадженні системи контролю за дотриманням політики кібербезпеки.

Отже, забезпечення на підприємстві достатнього рівня кібербезпеки вимагає комплексного підходу, в якому якісно організована система управління персоналом відіграє одну із найважливіших ролей.

Список використаних джерел:

1. Верезомська, І., Бовш, Л., Приходько, К., & Баклан, Х. (2022). Кіберзахист готельних брендів. *Ресторанний і готельний консалтинг. Інновації*, *5*(2), 190 -209. URL: https://doi.org/10.31866/2616-7468.5.2.2022.270089 (Дата звернення 05.10.2023)

2. Фостолович, В. А., Боцян, Т. В., Павлова, С. І. Штучний інтелект у сфері гостинності: місце інтегрування, специфіка використання та вплив на доходи підприємства. Економіка. Управління. Інновації. 2023. Випуск №2 (33). С. JEL Classification: O 320. DOI 10.35433/ISSN2410-3748-2022-2(31) URL: http://eprints.zu.edu.ua/id/eprint/37678 (Дата звернення 06.10.2023)