АНАЛІЗ СУЧАСНИХ ПІДХОДІВ ДО ОЦІНЮВАННЯ КІБЕРЗАГРОЗ ІНФОРМАЦІЙНИМ СИСТЕМАМ ПІДПРИЄМСТВ ІНДУСТРІЇ ГОСТИННОСТІ

Полотай Орест
к.т.н., доцент
Львівський державний університет безпеки життєдіяльності

Гарасимчук Олег
к.т.н., доцент
Національний університет Львівська політехніка

Полотай Богдана
старший викладач
Львівський торговельно-економічний університет

Сучасні підприємства індустрії гостинності широко впроваджують інформаційні технології з метою автоматизації ключових операційних процесів, підвищення якості обслуговування гостей та налагодження ефективної взаємодії з партнерами. Інформаційна інфраструктура готелів охоплює системи онлайн-бронювання, електронних платежів, програми лояльності, засоби контролю доступу, системи управління персоналом, відеоспостереження та різноманітні цифрові сервіси. Проте активна цифровізація готельної сфери одночасно розширює поверхню атаки, створюючи додаткові вразливості та підвищуючи ризик виникнення кіберзагроз [1].

Характерною рисою інформаційних систем підприємств індустрії гостинності є значний обсяг даних, які вони накопичують, обробляють і зберігають. Серед них особливе місце займають персональні відомості про гостей, платіжні реквізити, інформація щодо бронювання, дані про співробітників, внутрішні документи та інші службові відомості. Несанкціонований доступ до такої інформації або її компрометація можуть спричинити суттєві фінансові збитки, зниження рівня довіри з боку клієнтів, погіршення ділової репутації та порушення стабільної роботи готельного підприємства [2].

Враховуючи зазначене, одним із ключових завдань є своєчасне виявлення та оцінювання кіберзагроз для визначення рівня їхньої пріоритетності й забезпечення раціонального розподілу ресурсів, спрямованих на кіберзахист. Важливим аспектом при цьому є вибір відповідного підходу до оцінювання ризиків, адже визначення критичності загрози виключно на основі її технічних характеристик не завжди дає змогу врахувати особливості функціонування конкретного підприємства індустрії гостинності, його інформаційної інфраструктури та потенційні наслідки реалізації відповідної загрози [3].

Одним із найбільш поширених підходів до оцінювання технічної складової кіберзагроз є використання системи Common Vulnerability Scoring System (CVSS). Даний підхід дає змогу визначити рівень серйозності вразливості на основі стандартизованого набору характеристик. До них належать вектор атаки, складність атаки, необхідність привілеїв, взаємодія з користувачем, вплив на конфіденційність, цілісність та доступність інформації [4].

Значною перевагою CVSS є стандартизований характер оцінювання. Використання єдиної шкали дозволяє порівнювати різні вразливості між собою та визначати ті з них, які потребують першочергової уваги. Такий підхід є особливо корисним для систематизації великої кількості технічних вразливостей інформаційної інфраструктури [5].

Водночас застосування лише технічних методів оцінювання має певні обмеження. Високе значення CVSS не завжди свідчить про те, що відповідна загроза становить найбільшу небезпеку саме для конкретного підприємства індустрії гостинності. Наприклад, вразливість може характеризуватися високим технічним рівнем критичності, однак стосуватися ресурсу, який використовується незначною мірою або не містить важливої для готелю інформації. Натомість загроза з нижчим технічним показником може спричинити суттєвіші наслідки через особливості інформаційної інфраструктури, організації бізнес-процесів та залежності готелю від відповідних цифрових сервісів.

Важливе місце в оцінюванні кіберзагроз посідає ризик-орієнтований підхід, відповідно до якого рівень ризику визначається з урахуванням імовірності реалізації загрози та можливих наслідків її впливу. У загальному вигляді ризик можна розглядати як залежність між імовірністю виникнення небажаної події та масштабом потенційних збитків або інших негативних наслідків. Застосування такого підходу дає можливість перейти від ізольованого аналізу технічних характеристик вразливості до комплексного оцінювання її потенційного впливу на функціонування підприємства індустрії гостинності, його інформаційні ресурси та якість обслуговування клієнтів [6].

Для підприємств індустрії гостинності застосування ризик-орієнтованого підходу є особливо важливим, оскільки наслідки реалізації кіберзагроз можуть одночасно впливати на різні аспекти їхньої діяльності. Так, збої в роботі систем бронювання здатні спричинити фінансові втрати, порушення обслуговування та зниження рівня задоволеності гостей. Несанкціонований доступ до платіжної інформації може призвести до матеріальних збитків, витоку конфіденційних даних і погіршення ділової репутації підприємства. Водночас порушення функціонування систем контролю доступу може створювати безпосередню загрозу безпеці гостей, працівників та самого готельного об’єкта [7].

Водночас оцінювання ризику також залежить від якості вихідних даних. Визначення ймовірності реалізації загрози може бути складним за відсутності достатньої статистики щодо попередніх інцидентів. Крім того, оцінювання потенційних наслідків часто має суб'єктивний характер і залежить від експертних суджень [8].

Важливим чинником, який необхідно враховувати під час оцінювання сучасних кіберзагроз, є людський фактор. Працівники підприємств індустрії гостинності можуть бути потенційними цілями фішингових кампаній, атак із застосуванням методів соціальної інженерії, компрометації облікових записів та інших способів отримання несанкціонованого доступу до інформаційних систем.

У зв'язку з цим для підвищення об'єктивності оцінювання доцільно враховувати поведінкові характеристики кіберзагроз. До таких характеристик можна віднести складність реалізації атаки з урахуванням поведінки користувача, необхідність безпосередньої взаємодії зі співробітниками, можливість застосування методів соціальної інженерії, а також залежність результативності атаки від помилкових або необережних дій персоналу.

Урахування поведінкових параметрів дозволяє доповнити технічну оцінку інформацією щодо реальної ймовірності успішної реалізації кіберзагрози в конкретних умовах. Наприклад, фішингова атака може не характеризуватися високою технічною складністю, проте її ефективність значною мірою визначається рівнем обізнаності працівників, їхньою здатністю розпізнавати підозрілі повідомлення та дотриманням встановлених вимог інформаційної безпеки.

Таким чином, поведінкові характеристики доцільно виділяти в окрему групу параметрів, яка доповнює традиційні технічні показники та дає змогу точніше визначити реальний рівень небезпеки кіберзагрози для підприємства.

Не менш важливим напрямом удосконалення процесу оцінювання є врахування контексту функціонування інформаційної системи. Одна й та сама кіберзагроза може мати різний рівень критичності для різних підприємств індустрії гостинності залежно від особливостей їхньої інформаційної інфраструктури, використовуваних ресурсів, організації бізнес-процесів та ступеня залежності від цифрових технологій.

До контекстних характеристик можуть належати критичність інформаційного ресурсу, значущість пов'язаного з ним бізнес-процесу, кількість користувачів системи, рівень залежності підприємства від її безперебійної роботи, можливі фінансові та репутаційні втрати, а також вплив інциденту на безперервність надання готельних послуг.

Наприклад, порушення функціонування системи управління бронюванням у великому готельному комплексі може мати значно серйозніші наслідки, ніж аналогічний інцидент у невеликому готелі, який має можливість використовувати альтернативні канали приймання та обробки бронювань. Подібним чином компрометація системи контролю доступу може характеризуватися різним рівнем критичності залежно від ступеня її інтеграції з іншими елементами інформаційної та фізичної інфраструктури підприємства.

Отже, комплексне оцінювання кіберзагроз для підприємств індустрії гостинності доцільно здійснювати з урахуванням технічних, поведінкових і контекстних характеристик, що дозволяє отримати більш об'єктивну оцінку ризику та визначити пріоритетні напрями захисту інформаційної інфраструктури.

Таким чином, контекстна складова дозволяє перейти від універсального оцінювання загрози до оцінювання її фактичної значущості для конкретного підприємства.

Проведений аналіз показує, що сучасні підходи до оцінювання кіберзагроз мають як переваги, так і певні обмеження (таблиця 1).

Таблиця 1

Порівняльний аналіз сучасних підходів до оцінювання кіберзагроз

Підхід	Основна характеристика	Переваги	Основні обмеження
CVSS	Оцінювання технічної серйозності вразливості	Стандартизованість, об'єктивність, можливість порівняння	Не враховує специфіку конкретного підприємства
Ризик-орієнтований	Урахування ймовірності реалізації загрози та потенційних наслідків	Орієнтація на потенційні збитки та ризики для підприємства	Залежність від якості вихідних даних і експертних оцінок
Поведінковий	Врахування людського фактора та особливостей поведінки користувачів	Дає змогу враховувати соціальну інженерію, помилки персоналу та взаємодію з користувачем	Складність кількісного оцінювання поведінкових характеристик
Контекстний	Урахування особливостей конкретної інформаційної системи та бізнес-процесів	Відображає реальну значущість загрози для конкретного підприємства	Потребує детальної інформації про інформаційну систему та підприємство
Комплексний	Поєднання технічних, поведінкових і контекстних характеристик	Забезпечує більш повну та об'єктивну оцінку кіберзагрози	Потребує формалізації та узгодження різнорідних показників

Жоден із розглянутих підходів не забезпечує повного врахування всіх факторів, які визначають реальну небезпечність кіберзагрози для підприємства індустрії гостинності. Технічна оцінка є необхідною для визначення базового рівня серйозності, проте її доцільно доповнювати характеристиками, що відображають поведінкові та контекстні особливості.

З огляду на результати проведеного аналізу доцільним є використання комплексного підходу, який передбачає одночасне врахування технічної, поведінкової та контекстної складових кіберзагрози.

У такому випадку кожна кіберзагроза може бути представлена набором характеристик:

$$Y_i=\{T_i, B_i, K_i\} \quad (1)$$

де T_i – технічна складова, B_i – поведінкова складова, а K_i – контекстна складова і-ї кіберзагрози.

Для забезпечення можливості порівняння різнорідних характеристик їх необхідно привести до єдиної нормованої шкали. Наприклад, технічну складову, отриману на основі CVSS, можна нормувати за формулою:

$$T_i=CVSS_i/10 \quad (2)$$

Поведінкову та контекстну складові доцільно формувати на основі сукупності відповідних часткових показників. Після їх нормування може бути визначений інтегральний показник пріоритетності кіберзагрози:

$$R_i=\alpha T_i+\beta B_i+\gamma K_i \quad (3)$$

де: α, β, γ – вагові коефіцієнти відповідних складових. За умови однакової значущості складових:

$$\alpha=\beta=\gamma=1/3 \quad (4)$$

а інтегральна оцінка визначається як:

$$R_i=(T_i+B_i+K_i)/3 \quad (5)$$

Отримане значення дозволяє здійснювати порівняння різних кіберзагроз та формувати їх рейтинг за рівнем пріоритетності. При цьому загроза з найбільшим значенням (R_i) повинна розглядатися як така, що потребує першочергового застосування заходів кіберзахисту.

Застосування такого підходу є особливо актуальним для інформаційних систем підприємств індустрії гостинності, оскільки він дає змогу оцінювати кіберзагрози не лише за їхніми технічними характеристиками, а й з урахуванням поведінки користувачів та специфіки функціонування конкретного підприємства індустрії гостинності.

Таким чином, перспективним напрямом є формування комплексної моделі оцінювання кіберзагроз, яка поєднує технічні, поведінкові та контекстні параметри. Інтегрування зазначених складових у єдину систему оцінювання дозволяє здійснювати більш об’єктивне ранжування загроз за рівнем їхньої небезпечності та визначати пріоритетні напрями кіберзахисту. Це, у свою чергу, створює основу для раціонального розподілу ресурсів і більш обґрунтованого планування заходів із забезпечення безпеки інформаційних систем підприємств індустрії гостинності.

Список літератури

1. Полотай О., Кухарська Н., Полотай Б., Вітик Ю. Інформаційна безпека кіберфізичних систем як чинник якості послуг у готельно-ресторанному бізнесі. Кібербезпека: освіта, наука, техніка. 2026. DOI: 10.28925/2663-4023.2026.32.1103.

2. Orest Polotai, Bohdana Polotai, Oleh Harasymchuk, Natalia Kukharska Analysis of the state of information security at hotel and restaurant enterprises. Proceedings of the Workshop on Cyber Security and Data Protection (CSDP 2026). Lviv, Ukraine, May 7, 2026. P.154-171

3. ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024.

4. FIRST. Common Vulnerability Scoring System Version 4.0: Specification Document. Forum of Incident Response and Security Teams, 2024. URL: https://www.first.org/cvss/specification-document%2A%2A

5. FIRST. Common Vulnerability Scoring System Version 4.0: User Guide. Forum of Incident Response and Security Teams, 2024. URL: https://www.first.org/cvss/user-guide.htm

6. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. National Institute of Standards and Technology, 2024. DOI: 10.6028/NIST.CSWP.29.

7. ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection – Guidance on managing information security risks. Geneva: International Organization for Standardization, 2022.

8. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5. Gaithersburg: NIST, 2020.