УДК 004.056:005.334:658.5

Пухта В.М.

Шиян А.А.

SWOT-АНАЛІЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА НА ОСНОВІ РОМАНУ «ПАРК ЮРСЬКОГО ПЕРІОДУ»

Вінницький національний технічний університет

Анотація

У роботі проведено SWOT-аналіз тематичного парку з динозаврами як складної кіберфізичної системи, що поєднує комерційні, технологічні та інформаційно-безпекові аспекти. Досліджено сильні та слабкі сторони проєкту, а також визначено ключові можливості й загрози його функціонування в умовах високого рівня автоматизації та централізованого управління. Особливу увагу приділено ризикам, пов'язаним із людським фактором, надмірною централізацією, недостатнім контролем доступу та відсутністю ефективних механізмів резервування й моніторингу. На основі підходів ISO/IEC 27001 і сучасних принципів управління ризиками обґрунтовано необхідність впровадження багаторівневих систем захисту, децентралізації управління та підвищення стійкості до інцидентів. Отримані результати демонструють, що ефективне поєднання організаційних і технічних заходів є ключовим фактором забезпечення безпеки складних інфраструктурних об'єктів.

Ключові слова: *SWOT-аналіз, управління ризиками, інформаційна безпека, контроль доступу, кіберфізичні системи, кібербезпека.*

Abstract

This paper presents a SWOT analysis of a dinosaur-themed park as a complex cyber-physical system that combines commercial, technological, and information security aspects. The strengths and weaknesses of the project are examined, along with key opportunities and threats associated with its operation in a highly automated and centrally managed environment. Particular attention is paid to risks related to the human factor, excessive centralization, insufficient access control, and the lack of effective backup and monitoring mechanisms. Based on ISO/IEC 27001 approaches and modern risk management principles, the necessity of implementing multi-layered security systems, decentralization, and improved incident resilience is justified. The results demonstrate that an effective combination of organizational and technical measures is essential for ensuring the security of complex infrastructural systems.

Keywords: *SWOT analysis, risk management, information security, access control, cyber-physical systems, cybersecurity.*

Вступ

SWOT-аналіз – один із інструментів бізнес-управління, на якому ґрунтуються стратегічне планування, маркетинг та управління ризиками [1]. У сучасних умовах такий підхід доцільно застосовувати не лише до класичних підприємств, а й до складних технологічних систем, де ефективність функціонування залежить від рівня управління, автоматизації, захисту інформації та стійкості до внутрішніх і зовнішніх ризиків. Саме тому SWOT-аналіз є доречним для оцінювання проєкту тематичного парку з динозаврами компанії InGen, який у романі постає як високотехнологічне підприємство з централізованим керуванням, складною інфраструктурою та підвищеними вимогами до безпеки інформації і контролю доступу [2].

Вибір саме цього прикладу зумовлений тим, що у відкритих джерелах складно знайти настільки детально описане підприємство, яке одночасно поєднує комерційні, технологічні та безпекові аспекти. У романі М. Дж. Крайтона «Парк Юрського періоду» глибоко розкрито організацію роботи парку, його системи контролю доступу, моніторингу, автоматизації та управління, а також уразливості, пов'язані з людським фактором, централізацією й можливістю внутрішнього саботажу. Це створює зручну основу для SWOT-аналізу, у межах якого можна оцінити не лише бізнес-потенціал проєкту, а й його інформаційно-безпекові ризики, що є критично важливими для стабільного функціонування подібної системи.

Результати дослідження

Проведений SWOT-аналіз показав, що парк Юрського періоду у романі постає як унікальний, надзвичайно амбітний і водночас внутрішньо нестійкий проєкт, у якому високий рівень технологічності поєднується з критичною вразливістю до управлінських помилок і недосконалої організації контролю. З позиції стратегічної оцінки це не просто розважальний парк, а складна інтегрована система, де стабільність функціонування безпосередньо залежить від узгодженості технологічних рішень, надійності

інфраструктури, якості управління доступом та дисципліни персоналу. Саме поєднання інноваційності та недостатньої стійкості формує ключову суперечність проєкту, яка й визначає його подальший розвиток у межах сюжету. [2]

Стандарт ISO/IEC 27001 є одним із найбільш широко використовуваних та прийнятих стандартів інформаційної безпеки у світі [3]. Його логіка особливо доречна для аналізу подібного об'єкта, оскільки роман показує типові слабкі місця системи: надмірну централізацію, недостатній контроль доступу, слабке резервування та пізнє реагування на інциденти. Саме тому розгляд парку Юрського періоду крізь призму ISO/IEC 27001 дозволяє точніше побачити, яких саме управлінських і організаційних механізмів йому бракує для стабільної роботи.

Формування системи управління ризиками підприємства передбачає не лише виявлення загроз, а й їх системне оцінювання, пріоритизацію та вибір адекватних заходів реагування [4]. Для складних об'єктів особливо важливо поєднувати стратегічний аналіз із практичними інструментами контролю, адже саме така логіка дає змогу зменшувати наслідки інцидентів ще до того, як вони переростуть у кризу.

1) ***S – сильні сторони***

Найважливішою сильною стороною парку Юрського періоду є його абсолютна унікальність. Це перший у своєму роді проєкт, у межах якого відвідувачам демонструють живих динозаврів, створених за допомогою генетичних технологій. Така ідея формує надзвичайно сильний комерційний ефект, забезпечує глобальну увагу до проєкту та практично усуває пряму конкуренцію. З точки зору бізнесмоделі це рідкісний приклад продукту, який одночасно поєднує наукову новизну, видовищність і високий потенціал монетизації.

Ще однією сильною стороною є високий рівень технологічності. У романі парк функціонує як складна система, що спирається на клонування, автоматизоване керування, сенсорний моніторинг, електронний контроль і централізоване управління інфраструктурою [2]. За задумом це створює враження сучасного, добре організованого середовища, у якому більшість процесів можна контролювати з єдиного центру. Саме така архітектура підсилює масштабність проєкту й робить його привабливим як для інвесторів, так і для відвідувачів.

2) ***W – слабкі сторони***

Найсуттєвішою слабкою стороною парку Юрського періоду є надмірна залежність від технологій і централізованого керування. Якщо всі критичні процеси – від енергопостачання до охоронних механізмів – зосереджені в одному управлінському вузлі, будь-який збій одразу створює ефект доміно. У такій системі відмова однієї ланки здатна паралізувати весь об'єкт. Роман дуже чітко демонструє, що складна інфраструктура без достатнього резервування стає крихкою й легко втрачає стійкість у кризовий момент.

Другою слабкістю є залежність від людського фактора. Парк працює через людей, які мають доступ до критично важливих функцій, а отже, помилка, недбалість або навмисне втручання одного працівника можуть порушити весь механізм безпеки. Це свідчить про недостатньо чіткий розподіл повноважень, слабкий контроль доступу та відсутність надійних бар'єрів проти зловживання правами. У такій моделі внутрішній користувач стає не допоміжною ланкою, а однією з головних точок ризику. [2][3]

Третьою слабкою стороною є відсутність достатньо продуманих резервних сценаріїв. Для об'єкта такого масштабу необхідні дублюючі механізми управління, автономні режими роботи, окремі безпечні контури та можливість швидкого переходу в аварійний стан без повної втрати контролю [5]. Проте в романі видно, що система орієнтована переважно на нормальний режим функціонування, а не на кризовий. Саме тому навіть один збій або саботаж запускає ланцюг подій, які неможливо швидко зупинити.

3) ***O – можливості***

Як проєкт парк з тематикою динозаврів мав би величезні можливості для розвитку. У разі стабільного функціонування він міг би стати не лише туристичним об'єктом, а й платформою для науково-освітньої діяльності, міжнародного співробітництва, дослідницьких програм і комерційної експансії. Парк потенційно міг би перетворитися на цілу екосистему сервісів, що поєднує біотехнології, розваги та просвітництво.

Крім того, у найкращому сценарії така установа могла б закріпитися як символ інноваційного прориву, демонструючи можливості генетики, біоінженерії та сучасних систем контролю. Це створює можливість не просто продавати видовищність, а формувати образ прогресивного наукового центру. Водночас саме такі можливості вимагають максимально надійної внутрішньої організації, оскільки чим вищий рівень новизни й автоматизації, тим дорожчою стає будь-яка помилка.

4) ***T – загрози***

Найбільш очевидною загрозою є внутрішній саботаж. У романі саме втручання співробітника, який має легітимний доступ до систем, запускає критичні порушення в роботі парку. Це демонструє, що найбільша небезпека для подібного об'єкта походить не лише ззовні, а й із середини. Коли повноваження не

збалансовані, а контроль недостатньо жорсткий, один зловмисний крок може зруйнувати всю систему безпеки. [3]

Другою загрозою є надмірна централізація управління. Оскільки парк функціонує як єдина керована структура, збій у центральному вузлі автоматично створює кризу для всіх підсистем. Така архітектура робить об’єкт особливо вразливим до локальних відмов, цілеспрямованого втручання або компрометації окремого елемента [4]. У практичному сенсі це означає, що одна слабка точка може спричинити повний колапс.

Третьою загрозою є недостатній контроль доступу та можливість несанкціонованого впливу на критичні процеси. Коли права користувачів не розмежовані достатньо чітко, а система не має надійного механізму перевірки дій, навіть один обліковий запис може стати джерелом масштабної загрози. У такому середовищі ризик полягає не тільки в прямому зловживанні, а й у тому, що порушення може залишатися непоміченим до моменту, коли наслідки вже незворотні.

Ще однією серйозною загрозою є слабкий моніторинг та запізніле реагування. Система повинна виявляти аномалії до того, як вони перетворяться на інцидент великого масштабу, однак у романі проблеми стають помітними вже тоді, коли ситуація фактично виходить з-під контролю. Це показує, що відсутність якісного спостереження, журналювання й оперативного реагування є критично небезпечною для будь-якої складної інфраструктури.

Окрему загрозу становлять природні та зовнішні фактори, які можуть стати каталізатором уже наявних слабкостей [5]. У романі форс-мажор не є першопричиною катастрофи, але він різко погіршує умови та ускладнює відновлення контролю. Це доводить, що навіть зовнішня подія, яка сама по собі не є критичною, у поєднанні з поганою архітектурою може спричинити повну втрату стійкості системи.

Нарешті, до загроз належить і репутаційно-фінансовий колапс. Для об’єкта, який позиціонується як високотехнологічний і безпечний, втрата контролю означає не просто операційну помилку, а руйнування довіри, інвестиційної привабливості та самої моделі існування проєкту [4]. Отже, загроза полягає не лише у фізичному прориві системи, а й у знищенні її авторитету.

Висновки

У результаті дослідження було проведено SWOT-аналіз тематичного парку з динозаврами як складної кіберфізичної системи, що поєднує високий рівень технологічності, комерційний потенціал і підвищені вимоги до інформаційної безпеки. Встановлено, що ключова суперечність проєкту полягає у поєднанні інноваційності та масштабності з критичною залежністю від централізованого управління, людського фактора та недостатньо розвинених механізмів контролю і резервування. Аналіз дозволив виявити, що основні ризики формуються не лише технічними обмеженнями, а й організаційними недоліками, зокрема слабким розмежуванням доступу, відсутністю ефективного моніторингу та недостатньою готовністю до інцидентів.

Застосування підходів ISO/IEC 27001 та принципів управління ризиками показало, що підвищення стійкості подібних систем можливе за рахунок впровадження багаторівневого контролю доступу, децентралізації критичних процесів, розвитку систем раннього виявлення інцидентів і створення ефективних механізмів резервування. Комплексне поєднання технологічних рішень і управлінських підходів формує основу для побудови надійної та безпечної інфраструктури, здатної протидіяти як внутрішнім, так і зовнішнім загрозам. Подальші дослідження доцільно спрямувати на вдосконалення моделей управління ризиками, інтеграцію інтелектуальних систем моніторингу та розробку адаптивних механізмів реагування на інциденти в умовах високотехнологічних середовищ.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. SWOT-аналіз: сутність та особливості проведення. *DSpace Repository :: Репозитарій ПДАУ :: Головна*. URL: https://dspace.pdau.edu.ua/entities/publication/97a2840d-b2be-4d4a-bbd5-f9b634c7333c (дата звернення: 06.05.2026).
2. Крайтон М. Дж. "Парк Юрського періоду". Нью-Йорк : Alfred A. Knopf, 1990. 399 с.
3. Management of enterprise cyber security: A review of ISO/IEC 27001:2022. *IEEE Xplore*. URL: https://ieeexplore.ieee.org/abstract/document/10051114 (дата звернення: 06.05.2026).
4. ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ ПІДПРИЄМСТВА | Збірник наукових праць Таврійського державного агротехнологічного університету (економічні науки). *Фахові видання Таврійського державного агротехнологічного університету імені Дмитра Моторного*. URL: https://oj.tsatu.edu.ua/index.php/zbirnyk/article/view/863 (дата звернення: 06.05.2026).
5. LSULS Digital Repository: Інструментальні засоби управління ризиками у проектах безпечної експлуатації об’єктів масового перебування людей. *LSULS Digital Repository: Home*. URL: https://sci.ldubgd.edu.ua/jspui/handle/123456789/16374 (дата звернення: 06.05.2026).

Пухта Владислав Максимович – студент групи 2КІТС-24б, Вінницький національний технічний університет, м. Вінниця, vlad.puhta@gmail.com

Науковий керівник: Шиян Анатолій Антонович – кандидат фізико-математичних наук, доцент кафедри менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: anatoliy.a.shiyan@gmail.com.

Pukhta Vladyslav Maksymovych – student of group 2KITS-24b, Vinnytsia National Technical University, Vinnytsia, vlad.puhta@gmail.com

Supervisor: Shyian Anatolii Antonovych – PhD in Physical and Mathematical Sciences, Associate Professor at the Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: anatoliy.a.shiyan@gmail.com.