Загалом, успішна інтернет-стратегія вимагає комплексного підходу, де SEO та контент-маркетинг працюють разом для досягнення спільної мети — залучення та утримання клієнтів, підвищення впізнаваності бренду та збільшення конверсій. Постійний моніторинг, аналіз та адаптація до нових умов ринку дозволяють залишатися конкурентоспроможними та досягати довгострокового успіху.

Література:

1.Інформація про компанію «зроблено в україні "XYZ" TM». *"Зроблено в Україні "XYZ" TM" - контакти, товари, послуги, ціни*. URL: https://xyz.ua/ua/about_us (дата звернення: 07.11.2024).

2. Що таке контент-маркетинг: визначення, рекомендації | SendPulse UA. *SendPulse*. URL: https://sendpulse.ua/support/glossary/content-marketing (дата звернення: 07.11.2024).

3. Що таке SEO оптимізація сайту? Пояснюю простими словами!. *Bevisible*. URL: https://bevisible.com.ua/blog/scho-take-seo/ (дата звернення: 07.11.2024).

Горпинченко О.В.
кандидат економічних наук, доцент
Фрейдіс Р.В.
здобувач вищої освіти другого (магістерського) рівня
спеціальності 073 «Менеджмент» ОПП «Управління фінансово-економічною безпекою»
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

ЦИФРОВА БЕЗПЕКА: СУЧАСНІ ВИКЛИКИ ТА СТРАТЕГІЇ ЗАХИСТУ ІНФОРМАЦІЇ

У сучасному світі цифрові технології стали невід'ємною частиною повсякденного життя, проникаючи у всі сфери діяльності – від особистих фінансів до складних корпоративних систем. Разом з численними можливостями для розвитку та оптимізації бізнес-процесів, ці технології також відкривають нові виклики в сфері забезпечення безпеки інформації та захисту приватних даних.

Цифрова безпека, що охоплює захист комп'ютерних систем, мереж, програмного забезпечення та даних, стає одним з найбільш критичних аспектів для організацій і державних установ у всьому світі. З огляду на те, що зростає кількість кібератак, витоків даних і випадків крадіжки особистої інформації, питання цифрової безпеки набуває особливої актуальності. Проблеми кібербезпеки, такі як фішинг, віруси, шкідливе програмне забезпечення та зловмисний доступ до особистих даних, можуть мати серйозні економічні та репутаційні наслідки як для окремих користувачів, так і для цілих компаній.

Окрім того, цифрова безпека є ключовим фактором у забезпеченні стабільності цифрової економіки, яка активно розвивається в умовах глобалізації. Інститути і підприємства, що не приділяють належної уваги захисту своїх інформаційних ресурсів, можуть опинитися в ситуації, коли втратять не лише фінансові активи, але й довіру своїх клієнтів та партнерів.

Невід'ємною частиною цифрової безпеки є також освіченість користувачів: в умовах постійно зростаючої складності кіберзагроз важливо, щоб кожен користувач мав базові знання та навички для захисту своїх персональних даних і приватної інформації в інтернеті.

Іншим значним викликом є захист персональних даних, який набуває все більшої актуальності у світі, де дані є цінним ресурсом. Зростання кількості даних, що збираються через соціальні мережі, електронні платежі та інші онлайн-сервіси, відкриває нові можливості для витоків і крадіжок інформації. Порушення конфіденційності може призвести до значних юридичних та фінансових наслідків, а також підриву довіри до компаній і сервісів. На тлі цього також виникає необхідність дотримання суворих стандартів і законодавства щодо захисту персональних даних, як-от GDPR в Європейському Союзі.

Ще одним викликом є недостатня кіберосвіченість та обізнаність користувачів. Багато людей не знають основних принципів безпеки в Інтернеті, таких як правильне створення паролів, виявлення фішингових листів чи уникання підозрілих вебсайтів. Це робить їх вразливими до атак і може стати основною причиною витоків даних. Більше того, навіть у середовищі компаній недостатня увага до безпеки з боку працівників може призвести до серйозних порушень і витоків конфіденційної інформації.

Технічна складність сучасних інформаційних технологій також додає нові труднощі у сфері цифрової безпеки. Розвиток таких технологій, як Інтернет речей (IoT), 5G мережі, штучний інтелект та блокчейн, створює нові точки вразливості, які можна використовувати для атак. Підключення великої кількості пристроїв до Інтернету або перехід на нові стандарти зв'язку й шифрування потребують постійного оновлення методів захисту та адаптації інфраструктури.

Крім того, цифрова безпека стикається з проблемами, пов'язаними з міжнародною співпрацею та кіберзлочинністю. Кіберзлочинці все частіше працюють на глобальному рівні, а закони та стандарти в різних країнах можуть суттєво відрізнятися. Це ускладнює міжнародну координацію у боротьбі з кіберзлочинцями, адже ефективна боротьба потребує спільних зусиль і обміну інформацією між країнами. Виклики, пов'язані з кіберзлочинністю, також включають труднощі у виявленні та покаранні правопорушників, оскільки вони можуть здійснювати свої дії анонімно через складні мережі і системи.

Стратегії подолання цифрової небезпеки вимагають комплексного підходу, що включає як технічні, так і організаційні заходи. Для забезпечення належного рівня цифрової безпеки необхідно зосередитися на кількох ключових напрямках, серед яких: удосконалення технологічних рішень, підвищення рівня обізнаності користувачів, посилення політик щодо захисту даних і розвитку міжнародної співпраці.

По-перше, удосконалення технологій безпеки є основою для ефективного захисту від цифрових загроз. Використання шифрування даних, багатофакторної аутентифікації, систем виявлення вторгнень та новітніх методів захисту від вірусів допомагає створювати захищене середовище для збереження конфіденційності та цілісності даних. Важливо регулярно оновлювати програмне забезпечення та застосовувати патчі безпеки, щоб закривати вразливості систем. Крім того, підприємствам та організаціям слід інвестувати в інструменти для моніторингу кіберзагроз, щоб оперативно виявляти та нейтралізувати потенційні атаки.

По-друге, підвищення рівня кіберосвіченості серед користувачів є одним з основних напрямків у боротьбі з цифровими загрозами. Організації повинні регулярно проводити тренінги та семінари для своїх співробітників щодо основ цифрової безпеки: правильного створення паролів, розпізнавання фішингових атак, управління особистими даними та використання безпечних з'єднань. Для звичайних користувачів важливо надавати інформацію щодо базових принципів онлайн-безпеки, таких як уникання підозрілих посилань, регулярне оновлення паролів та обережність при використанні публічних Wi-Fi мереж.

Третім важливим аспектом є посилення політик щодо захисту персональних даних. З огляду на численні випадки витоків та крадіжок даних, компанії повинні забезпечити відповідність своїх політик безпеки міжнародним стандартам, таким як GDPR (Загальний регламент захисту даних) в Європейському Союзі. Це включає в себе не тільки технічні заходи, а й чітке визначення правил зберігання, обробки та передачі персональних даних, а також швидке реагування на інциденти з порушенням безпеки.

Не менш важливою є міжнародна співпраця у сфері кібербезпеки. Кіберзлочинці часто діють на глобальному рівні, і для ефективного протистояння цим загрозам необхідно координувати зусилля між різними країнами, міжнародними організаціями та приватними компаніями. Спільне розроблення стандартів безпеки, обмін інформацією про нові загрози та координація дій при кіберінцидентах можуть значно підвищити ефективність боротьби з кіберзлочинністю.

Узагальнюючи можна дійти висновку, що боротьба з цифровою небезпекою потребує багатогранного підходу, що включає технологічні інновації, регулярне навчання

користувачів, чіткі політики захисту даних та активну міжнародну співпрацю. Тільки в комплексі ці стратегії можуть забезпечити належний рівень безпеки в умовах, коли кіберзагрози стають дедалі більш складними та масштабними. Важливо не лише впроваджувати ці стратегії, а й постійно адаптувати їх до нових викликів, оскільки сфера цифрової безпеки є надзвичайно динамічною і змінюється разом з технологічними інноваціями та розвитком нових видів кіберзагроз.

Література:

1. Samofalova, M., Horpynchenko, O., & Lytvyn, O. (2024). Financial provision of marketing activities of machine-building enterprises for strengthening competitiveness in the context of a new reality. *Financial and Credit Activity: Problems of Theory and Practice, 5*(58), 264–276. https://doi.org/10.55643/fcaptp.5.58.2024.4555 https://fkd.net.ua/index.php/fkd/article/view/4555

Горпинченко О.В.
кандидат економічних наук, доцент
Яцун В.В.,
кандидат технічних наук, доцент
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

CURRENT TRENDS AND FEATURES OF CONSTRUCTION MANAGEMENT IN THE ERA OF DIGITAL TRANSFORMATION

The relevance of digitalization in construction management is driven by several key factors that impact the efficiency and competitiveness of the industry.

The construction sector faces numerous challenges, such as rising costs, a shortage of skilled labor, project delays, and declining quality. Digitalization enables process optimization, cost reduction, and improved work quality. The use of technologies like Building Information Modeling, automation of design and construction, and project management systems enhances resource management and project scheduling efficiency.

Rapid changes in the technological landscape require companies to adopt new tools and working methods. Digital technologies such as artificial intelligence, big data, and the Internet of Things enable real-time data analysis, leading to better-informed management decisions. This, in turn, allows for quicker responses to market changes, improved strategic planning, and adaptation to new challenges [1].

Digitalization also supports sustainability and environmental responsibility in construction. Modern digital solutions help monitor resource use, reduce waste, and improve energy efficiency. For example, energy consumption monitoring systems allow for identifying inefficiencies and making adjustments during the design and operational phases of buildings.

Recently, there has been increased focus on collaboration among all construction process participants. Digital platforms provide real-time information exchange, which increases transparency and reduces the risk of errors. This fosters better coordination among architects, engineers, contractors, and clients, ultimately improving project outcomes.

Digitalization in construction management is an essential step toward enhancing efficiency, adaptability, and sustainability in the face of contemporary challenges. It unlocks new opportunities for innovation, increased competitiveness, and the creation of safer and more comfortable living environments in new buildings [2].

Integration of digital platforms for collaboration among all project participants. These platforms enable real-time information exchange, enhancing coordination and reducing errors. This approach improves communication between architects, engineers, contractors, and clients, increasing transparency and efficiency in construction projects.