Вплив інформаційних технологій на національну безпеку в умовах

глобалізаційних процесів в економіці

The Impact of Information Technology on

National Security in the Context of

Globalization Processes in the Economy

***Тараненко Юрій В’ячеславович***, студент,

Харьківський технологічний університет «ШАГ», м.Харків

***Науковий керівник: Задерей Юрій Миколайович***

Харьківський технологічний університет «ШАГ», м.Харків

У сучасному світі глобалізація змінює структуру економік, суспільств і держав, створюючи нові можливості та виклики. Інформаційні технології (ІТ) стають ключовим фактором у цих трансформаціях, відіграючи важливу роль у розвитку економіки та забезпеченні національної безпеки. Мета цього дослідження — виявити, як саме ІТ впливають на національну безпеку в умовах глобалізації, та запропонувати шляхи мінімізації ризиків.

Роль інформаційних технологій в економічній безпеці

Інформаційні технології сприяють підвищенню продуктивності праці, оптимізації виробничих процесів та розвитку нових секторів економіки, таких як електронна комерція та фінансові технології (FinTech). Наприклад, цифрові платформи значно спрощують міжнародну торгівлю, зменшуючи витрати та час на здійснення транзакцій [1]. Проте, зростаюча залежність від ІТ робить економіку вразливою до кібератак, зокрема атак на фінансові системи та критичну інфраструктуру. Наприклад, атаки на банківські системи можуть призвести до значних фінансових втрат та дестабілізації економічного сектору. Відомі

випадки, такі як злам SWIFT у 2016 році, підкреслюють важливість захисту фінансових систем [2].

# Кібератаки як загроза національній безпеці

З розвитком глобалізації збільшується кількість та складність кібератак. Вони можуть бути спрямовані на державні установи, критичну інфраструктуру, приватні компанії та навіть окремих громадян. Нещодавні атаки на енергетичні системи, такі як атака на Colonial Pipeline у 2021 році, демонструють, як кібератаки можуть спричиняти значні економічні та соціальні збитки [3]. Для ефективного захисту необхідно розробляти та впроваджувати сучасні методи кібербезпеки, включаючи системи моніторингу, виявлення та реагування на загрози. Використання штучного інтелекту для аналізу великих даних може значно підвищити ефективність виявлення та реагування на кібератаки [4].

# Захист конфіденційної інформації

В умовах глобальної конкуренції захист комерційних та державних секретів є пріоритетним завданням.

Використання сучасних криптографічних методів, таких як асиметрична криптографія та блокчейн-технології, може

забезпечити високий рівень безпеки даних [5]. Наприклад, технологія блокчейн може використовуватися для захисту фінансових транзакцій та запобігання шахрайству. Крім

того, системи управління доступом, такі як багатофакторна аутентифікація, є необхідними для запобігання несанкціонованого доступу до конфіденційної інформації

[6].

# Регуляторні аспекти та міжнародна співпраця

Ефективна боротьба з кіберзагрозами потребує не лише внутрішніх заходів, але й активної міжнародної співпраці. Створення глобальних стандартів та нормативно-правових актів, спрямованих на кібербезпеку, є важливим кроком до посилення колективної безпеки. Наприклад, угоди між

країнами щодо обміну інформацією про кіберзагрози та спільних навчань можуть значно підвищити рівень

готовності до кіберінцидентів [7]. Ініціативи, такі як Будапештська конвенція про кіберзлочинність, є важливими кроками у створенні міжнародної правової бази для боротьби з кіберзагрозами [8].

Інновації та розвиток технологій як інструмент безпеки:

Інвестиції в інноваційні ІТ-рішення, такі як штучний інтелект (ШІ), блокчейн та Інтернет речей (IoT), можуть стати ефективними інструментами для підвищення рівня національної безпеки. Наприклад, використання ШІ для аналізу великих даних дозволяє швидко виявляти аномалії та потенційні загрози, а блокчейн забезпечує прозорість та захист транзакцій [9]. Інтернет речей, з іншого боку, може допомогти в моніторингу та управлінні критичною інфраструктурою, забезпечуючи її безперебійне функціонування [10]. Розвиток таких технологій вимагає постійного оновлення знань та навичок спеціалістів у сфері ІТ та кібербезпеки.

**Література**:

1. "Цифрова економіка та суспільство в Україні: тенденції та перспективи розвитку" [Електронний ресурс]. – Режим доступу:

https://niss.gov.ua/doslidzhennya/ekonomika/cifrova-ekonomika-tasuspilstvo-v-ukraini-tendencii-ta-perspektivi-rozvitku.

1. "Захист банківської системи України в умовах кіберзагроз" - https://bank.gov.ua/admin\_uploads/article/Cyber\_security\_2021.pdf.
2. "Кіберзагрози в Україні: стан та перспективи розвитку" - https://niss.gov.ua/doslidzhennya/nacionalnabezpeka/kiberzagrozi-v-ukraini-stan-ta-perspektivi-rozvitku.
3. "Використання штучного інтелекту в кібербезпеці: перспективи та виклики" - https://cybersecurity.org.ua/use-ai-cybersecurity/.
4. "Блокчейн та його застосування в кібербезпеці” – https://itukraine.org.ua/blockchain-applicationcybersecurity.html.
5. "Управління доступом до інформаційних ресурсів: нові підходи та технології" –https://itd.rada.gov.ua/upload/documents/2018/2459.pdf.