КІБЕРБЕЗПЕКА ТА СТАНОВЛЕННЯ ЦИФРОВОЇ ЕКОНОМІКИ: ПРОБЛЕМИ ВЗАЄМОЗВ'ЯЗКУ

Страпчук С.І., канд. екон. наук, доц.
Харківський національний університет ім. В.Н. Каразіна
Остапенко Р.М., канд. екон. наук, доц.
Державний біотехнологічний університет

Цифрова економіка відіграє дедалі важливішу роль у нашому сучасному житті, проникаючи в різні сфери діяльності, від бізнесу до державного управління. Одночасно зі швидким розвитком цифрових технологій і старінням залежно від країн відкриваються простори для нових атак і викликів у сфері кібербезпеки.

Нині життя переходить в онлайн-простір, і цифрова економіка відіграє дедалі важливішу роль у розвитку суспільства. Однак із появою кількості цифрових послуг і можливостей також зростає і кількість кіберзагроз. Таким чином, кібербезпека стає резервним фактором, що сприяє розвитку цифрової економіки. Без належної уваги захисту від кібератак і загроз безпеки цифрова економіка ризикує постраждати.

З кожним роком все більше людей і підприємств проникають в ідеї цифрової трансформації.

Завдяки онлайн-покупкам у хмарних сервісах цифровізація стає частиною повсякденного життя. Однак зростання цифровізації також впливає на вплив технологій і збільшує вразливість для кібератак. Таким чином, зростання цифрової економіки вимагає активного і різнобічного підходу до кібербезпеки.

На жаль, зростання цифрової економіки неминуче привертає увагу зловмисників, які бажають отримати несанкціонований доступ до цифрових даних та інформації. Кіберзагрози, такі як конкурентні програми, рибна ловля, кібератаки та захист даних, стають дедалі поширенішими. У результаті, якщо не приділяти уваги кібербезпеці, цифрова економіка стикається з основними ризиками, які можуть завдати шкоди бізнесу і суспільству.

Однією з найбільш тривожних загроз у сфері цифрової економіки є масштабні кібератаки на критичну інфраструктуру. Кіберзлочинці можуть націлюватися на енергетичні системи, транспортні мережі, фінансове господарство та інші життєво важливі системи, що може призвести до серйозних наслідків для суспільства та економіки.

Кіберзлочини, такі як кібершахрайство і захист даних, також становлять серйозну загрозу для цифрової економіки. Витік конфіденційної інформації та клієнтських даних може завдати шкоди репутації компанії та підірвати довіру користувачів до цифрових сервісів.

Щоб цифрова економіка мала стійке зростання, кібербезпека має розглядатися як один із незалежних аспектів. Ефективні заходи захисту від кібератак, забезпечення конфіденційності даних та захист - все це є частиною основних факторів, що визначають успіх цифрової економіки.

У сьогоднішню цифрову епоху, коли економіка значною мірою залежить від технологій і взаємопов'язаних систем, забезпечення кібербезпеки має першорядне значення. Уряди відіграють вирішальну роль у захисті цифрової інфраструктури та створенні безпечного середовища для приватних осіб, підприємств і економіки в цілому.

Для вирішення зростаючих проблем кібербезпеки уряди в усьому світі розробили стратегії та політику, спеціально призначені для захисту від кіберзагроз. Ці стратегії спрямовані на підвищення стійкості критично важливої інфраструктури, сприяння обміну інформацією та співпраці між державним і приватним секторами, а також сприяння інноваціям у технологіях кібербезпеки.

За допомогою цих стратегій уряди прагнуть створити комплексні механізми, які усунуть не тільки поточні кіберризики, а й майбутні загрози в цифровому ландшафті, що постійно змінюється. Беручи активну участь у формуванні політики кібербезпеки, уряди можуть ефективно знижувати ризики, захищати національні інтереси і сприяти зростанню цифрової економіки.

У взаємопов'язаному світі цифрової економіки співпраця між урядом і приватним сектором має життєво важливе значення. Уряд володіє регулюючими і законодавчими повноваженнями, а приватний сектор володіє технічними знаннями і ресурсами, необхідними для ефективної боротьби з кіберзагрозами.

Створення партнерських відносин між цими двома організаціями дозволяє обмінюватися інформацією, передовим досвідом і ресурсами для підвищення можливостей кібербезпеки. Уряди можуть надавати стимули і створювати механізми, які заохочують участь приватного сектору в захисті критично важливої інфраструктури та конфіденційних даних. Водночас приватний сектор може зробити свій внесок, обмінюючись інформацією про загрози, допомагаючи в реагуванні на інциденти і беручи участь у спільних дослідженнях і розробках.

Крім того, співпраця між урядом і приватним сектором дає змогу розробляти надійні стандарти і правила кібербезпеки, які є практичними, ефективними і адаптованими до нових технологій. Працюючи разом, ці зацікавлені сторони можуть створити більш безпечне цифрове середовище, яке захищатиме як національні інтереси, так і економічне зростання.

Кібербезпека – це спільна відповідальність, і окремі особи також відіграють важливу роль у захисті цифрової екосистеми. Уряди визнали важливість ініціатив з освіти та підвищення обізнаності в галузі кібербезпеки, щоб надати громадянам знання та навички для захисту себе в цифровій сфері.

За допомогою інформаційних кампаній, освітніх програм і державно-приватного партнерства уряди можуть просувати культуру кібербезпеки. Ці ініціативи спрямовані на інформування людей про поширені кіберзагрози, безпечні методи роботи в Інтернеті та важливість оновлення систем і пристроїв за допомогою оновлень безпеки. Надаючи людям необхідні знання, уряди можуть створити більш стійке суспільство, яке зможе ефективно виявляти кіберзагрози та реагувати на них. Крім того, освіта в галузі кібербезпеки може сприяти кар'єрному зростанню в цій галузі, сприяючи зростанню кваліфікованої робочої сили, здатної вирішувати зростаючі проблеми цифрової економіки.

Хоча забезпечення кібербезпеки має вирішальне значення, не менш важливо знайти баланс між заходами безпеки і захистом прав на недоторканність приватного життя. Уряди повинні розробити політику, яка захищає як особисту конфіденційність, так і інтереси національної безпеки.

В епоху, коли персональні дані стають дедалі ціннішими, урядам необхідно створити законодавчу базу, яка захистить права людей на недоторканність приватного життя, одночасно забезпечуючи ефективні заходи кібербезпеки. Це може включати в себе впровадження правил захисту даних, забезпечення прозорості в зборі та використанні даних, а також забезпечення належного нагляду за діяльністю з нагляду.

Пошук правильного балансу між безпекою та конфіденційністю - це постійне завдання, що вимагає постійного діалогу між урядами, громадянським суспільством та експертами в галузі технологій. Вирішуючи ці проблеми і включивши заходи захисту конфіденційності в стратегії кібербезпеки, уряди можуть вселити суспільну довіру і впевненість у цифрову економіку.

Насамкінець зазначимо, що роль держави в забезпеченні кібербезпеки в умовах цифрової економіки багатогранна. Розробляючи надійні стратегії та політику, сприяючи співпраці з приватним сектором, просуваючи освіту в галузі кібербезпеки та розв'язуючи проблеми конфіденційності, уряди можуть створити безпечне та стійке цифрове середовище, яке сприятиме зростанню цифрової економіки.

У цифрову епоху забезпечення кібербезпеки стає частиною успіху в розвитку цифрової економіки. Необхідно дотримуватися консервативних підходів і заходів, вжитих як економічними, так і бізнесом, для захисту від кіберзагрози та забезпечення безпечного використання цифрових технологій. Тільки тісна співпраця та спільні зусилля всіх країн світу можуть забезпечити стабільність і надійність у цифровій економіці. Майбутня цифрова економіка залежить від нашої здатності ефективно боротися з кібербезпекою.

СИСТЕМИ АВТОМАТИЗАЦІЇ ВИРОБНИЦТВА СІЛЬГОСППРОДУКЦІЇ ТА НАДІЙНІСТЬ ЇХ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Чередниченко А.Є., здоб. вищої освіти
Шило Д.А., здоб. вищої освіти
Піскачова І.В., канд. техн. наук, снс
Державний біотехнологічний університет

Автоматизація виробничих процесів є технічним підґрунтям для розвитку різних напрямків промисловості та виробництва, в тому числі - в галузі сільського господарства та виробництва продуктів харчування. За останні роки істотно змінилися склад і структура технічних засобів, що застосовуються в автоматизованих системах управління технологічними процесами (АСУ ТП) у сільському господарстві. Сучасні АСУ ТП створюються на основі локальних