



**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»**



**НАВЧАЛЬНО-НАУКОВИЙ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ**



THEORETICAL AND APPLIED CYBERSECURITY

**Матеріали IV Всеукраїнської
науково-практичної конференції**

Випуск 4



Київ – 2026

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ
ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ
ІНСТИТУТ**

**THEORETICAL AND APPLIED
CYBERSECURITY**

**Матеріали IV Всеукраїнської
науково-практичної конференції**

Випуск 4

Київ – 2026

*Рекомендовано до друку Вченою радою
НН ФТІ КПІ ім. Ігоря Сікорського
(протокол № 9 від 29 червня 2026 р.)*

Theoretical and Applied Cybersecurity. Матеріали IV Всеукраїнської науково-практичної конференції (TACS-2026). – Київ: Інжиніринг. – 186 с. ISBN 978-617-8180-08-9

До збірника увійшли матеріали доповідей, представлених на IV Всеукраїнській науково-практичній конференції Theoretical and Applied Cybersecurity (TACS-2026, 28 травня 2026 р., м. Київ, Україна).

У збірнику представлені матеріали, присвячені питанням безпечного функціонування кібернетичного та інформаційного простору, безпеки промислових систем та систем критичної інфраструктури, математичних і технічних проблем кібернетичної безпеки, запобігання і протидії кібератакам, моделювання та протидії інформаційним операціям, технологій інформаційно-аналітичних досліджень на основі відкритих джерел інформації, застосування штучного інтелекту.

Для фахівців в області інформаційних технологій, інформаційної і кібернетичної безпеки, а також для аспірантів і студентів старших курсів вищої школи відповідних спеціальностей.

Редакційна колегія:

*О.М. Новіков, д.т.н., професор, член-кор. НАН України;
Д.В. Ланде, д.т.н., професор; С.А. Смирнов, к.т.н., с.н.с.;
А.Ш. Апішева, к.психол.н.; А.В. Напрєнко*

ISBN 978-617-8180-08-9

© НН ФТІ
КПІ ім. Ігоря Сікорського,
2026

© Колектив авторів, 2026

КОНФЛІКТОЛОГІЯ АВТОНОМНОГО ІІІ В ДЕРЖАВНИХ ЦИФРОВИХ ЕКОСИСТЕМАХ: РИЗИКИ ДОМІНУВАННЯ ТА УМОВИ СТРУКТУРНОЇ СТІЙКОСТІ

Ланде Д.В.¹, Даник Ю.Г.²

¹ КІІІ ім. Ігоря Сікорського, ORCID: 0000-0003-3945-1178,
dwlande@gmail.com.

² КІІІ ім. Ігоря Сікорського, ORCID: 0000-0001-6990-8656,
y.danik@gmail.com.

Актуальність дослідження зумовлена трансформацією державних цифрових сервісів з інструментів надання послуг у інфраструктуру примусової інтеграції. Насичення цих платформ алгоритмами штучного інтелекту (ІІІ) прискорює делегування рішень, породжуючи дві взаємопов'язані загрози: структурне домінування над користувачем з ерозією його агентності та різке зростання системної кібервразливості через централізацію даних і автономізацію виконавчих компонент. Мета роботи – формалізувати динаміку цих процесів, математично обґрунтувати умови катастрофічної розбіжності та запропонувати архітектурні стабілізатори, що трансформують систему на асимптотично стійку. Дослідження спирається на принципи кібернетичного регулювання, теорію динамічних систем та аналіз меж делегування рішень, уникаючи нормативних конструктів на кшталт «вбудованої етики».

Ключові слова: інтегровані цифрові платформи, штучний інтелект, алгоритмічне управління, конфліктологія ІІІ, структурна стійкість, архітектурні обмеження, математичне моделювання, цифрова агентність, кібербезпека

Вступ

Актуальність дослідження зумовлена трансформацією державних цифрових сервісів з інструментів надання

послуг у інфраструктуру примусової інтеграції. Насичення цих платформ алгоритмами штучного інтелекту (ШІ) прискорює делегування рішень, породжуючи дві взаємопов'язані загрози: структурне домінування над користувачем з ерозією його агентності та різке зростання системної кібервразливості через централізацію даних і автономізацію актуаторів.

Мета роботи – формалізувати динаміку цих процесів, математично обґрунтувати умови катастрофічної розбіжності та запропонувати архітектурні стабілізатори, що трансформують систему на асимптотично стійку. Дослідження спирається на принципи кібернетичного регулювання, теорію динамічних систем та аналіз меж делегування рішень, уникаючи нормативних конструктів на кшталт «вбудованої етики».

Дослідження спирається на принципи кібернетичного регулювання [1, 2], теорію динамічних систем [3, 4], класичні моделі розподілу контролю, делегування рішень [5,6]. Крім того, ця робота розвиває напрямок дослідження конфліктології ШІ [7-8].

Аналітичний каркас

Примусово інтегровану цифрову екосистему доцільно розглядати як замкнутий контур із трьома функціональними шарами: обов'язковий збір даних, алгоритмічна обробка та актуаторний вплив. Ключовий механізм дестабілізації – позитивний зворотний зв'язок між масштабом інтеграції, автономією ШІ та глибиною залежності громадянина. При функціонуванні декількох платформ виникає перехресна інтерференція: кожна система оптимізує власний функціонал, генеруючи суперечливі сигнали для одного об'єкта управління. Без протоколів арбітражу конфліктологія ШІ перетворюється на «війну оптимізаторів», а спільна кіберінфраструктура нелінійно розширює поверхню атаки. Таким чином, домінування та кібервразливість мають спільну математичну природу – необмежену позитивну петлю зворотного зв'язку.

Додатковим фактором дестабілізації є кібербезпека: централізовані високоавтономні системи мають нелінійно зростаючу поверхню атаки. Деструктивний вплив конкуруючих систем, компрометація ключів доступу або технічний злам перетворюється не на локальні помилки, а на каскадні тригери, що миттєво підсилюють контрольні сигнали або блокують критичні функції.

Математична модель

Для формалізації динаміки введемо змінні:

$s_i(t) \in \mathbb{R}_{\geq 0}$ – інтенсивність контролю i -ї платформи над цільовою аудиторією;

$a_i(t) \geq 1$ – рівень автономії ШІ;

$v_i(t) \in [0, 1]$ – індекс кібернетичної вразливості (ймовірність реалізації інциденту або впливу сигналу від конкурентів).

Розглянемо дві взаємодіючі системи ($i = 1, 2$). Базова динаміка описується:

$$\dot{s}_i = \mu a_i s_i + \gamma \omega_{ij} (s_j - s_i) + \xi_i v_i,$$

$$\dot{a}_i = \kappa s_i a_i,$$

$$\dot{v}_i = \alpha s_i a_i - \beta v_i,$$

де $\mu > 0$ – коефіцієнт перетворення даних у контроль; γ – сила міжсистемної взаємодії; $\omega_{ij} \in [-1, 1]$ – міра конфліктності ($\omega_{ij} < 0$ означає конкурентну оптимізацію);

$0 < \kappa > 0$ – швидкість зростання автономії; ξ_i – чутливість систем до кіберінцидентів; α – коефіцієнт зростання вразливості з централізацією та автономією; β – швидкість відновлення систем. Індекс агентності користувача обернено пропорційний середньому контролю:

$$A(t) = A_0 / \left(1 + \frac{s_1 + s_2}{2} \right).$$

Для ізольованої платформи ($\gamma = 0$, $\xi_i = 0$) система зводиться до $\dot{s} = \mu \kappa s^2$. Інтегрування дає розв'язок:

$$s(t) = \frac{s_0}{1 - \mu \kappa s_0 t},$$

який демонструє скінченночасову розбіжність (finite-time blow-up) при $t_c = (\mu \kappa s_0)^{-1}$. Це математичний еквівалент системного колапсу: контроль стає нескінченним за скінченний час, агентність $A(t) \rightarrow 0$. Додатково, $\dot{v}_i = \alpha s_i a - \beta v_i$ при $s_i, a \rightarrow \infty$ призводить до $v_i \rightarrow 1$, що означає повну кібернетичну відкритість. Будь-який зовнішній тригер $\xi_i > 0$ миттєво дестабілізує актуатори. У випадку двох конфліктних платформ ($\omega_{12} = \omega_{21} = -\omega < 0$) виникає осциляторна нестабільність з експоненціальним зростанням амплітуди, що моделює «війну алгоритмів» за статус користувача, підсилену кібернетичною взаємною експозицією – архітектурну та інформаційну взаємозалежність цифрових платформ.

Щоб уникнути розбіжності та кібернетичного колапсу, вводимо три архітектурні поправки:

1. Жорсткий ліміт автономії $a_i \leq a^*$.
2. Процедурна інерція (людський контур) – нелінійне сповільнення актуаторного впливу.
3. Протокол міжсистемного узгодження та ізоляції інцидентів:

Повна модифікована система має вигляд:

$$\dot{s}_i = \frac{\mu a_i s_i}{1 + \rho s_i} + \gamma \omega_{ij} (s_j - s_i) - \eta s_i (s_j - s_i)^2 + \xi_i v_i - \delta v_i s_i,$$

$$\dot{a}_i = \kappa s_i a_i - \lambda (a_i - a^*) \Theta(a_i - a^*),$$

$$\dot{v}_i = \alpha s_i a_i - \beta v_i.,$$

де a^*, λ – технічний ліміт автономії; ρ – процедурна інерція; η – протокол узгодження; δ – автоматичний кіберзапобіжник; $\Theta(\cdot)$ – функція Хевісайда.

Аналіз стійкості в симетричному випадку ($\omega_{12} = \omega_{21} = -\omega$) дає умови асимптотичної стабільності:

$$\rho\alpha^* > 1, \lambda > \kappa^*, \eta + \frac{\delta\alpha^*}{\beta} > |\gamma\omega|.$$

Виконання цих нерівностей гарантує єдину додатну точку рівноваги та перетворення розбіжної спіралі у стійкий вузол, де агентність $A(t) > 0$, а кіберінциденти не викликають каскадного зростання контролю.

Концептуальний сценарій та результати

За відсутності поправок ($\eta=0$, $\rho=0$, $\lambda \rightarrow \infty$, $\delta=0$) алгоритми вступають у конфлікт, індекс користувача осцилює, системи споживають ресурси на перерахунок. Користувач позбавлений альтернативних каналів, його агентність $A(t)$ наближається до нуля. Одночасно зростає v_i . Спеціально підготовлений сигнал для обману моделі або технічний злам ($\xi_i > 0$) миттєво підсилює контрольні сигнали, блокуючи рахунки та медичні записи. Модель демонструє скінченночасову розбіжність $s_i(t) \rightarrow \infty$, $A(t) \rightarrow 0$, що відповідає системному «заморожуванню» та кібернетичному колапсу.

Впровадження поправок змінює траєкторію: $a_i \leq a$ запобігає остаточним автоматичним рішенням; ρ вводить буфер для оскарження та перевірки під час тривоги; δ при зростанні v_i автоматично переводить систему в режим «обмеженого впливу», а η ініціює арбітраж між платформами. Користувач отримує статус «тимчасова валідація», системи стабілізуються навколо $s \approx 1/\rho$, агентність зберігається, кіберінцидент локалізується. Катастрофа замінюється керованою напругою з вбудованими механізмами відновлення.

Висновки

Примусово інтегровані цифрові екосистеми, насичені автономним ІШ, без архітектурних обмежень демонструють скінченночасову розбіжність, що математично моделює одночасну втрату людської агентності та каскадний кібернетичний колапс. Доведено, що цей ефект є не наслідком програмних помилок чи

недосконалості алгоритмів, а фундаментальною властивістю динамічних систем. Введення трьох інженерних стабілізаторів – жорсткого ліміту автономії (α^*, λ), процедурної інерції (ρ) та протоколу міжсистемного узгодження з автоматичним кіберзапобіжником (η, δ) – трансформує фазовий простір системи, перетворюючи розбіжну динаміку на асимптотично стійку. Аналітично виведені умови стійкості

$(\rho\mu\alpha^* > 1, \lambda > k\sigma^*, \eta + \delta\alpha\alpha^*/\beta > |\gamma\omega|)$ отримують чітку

технічну інтерпретацію. Модель вперше формально пов'язує втрату агентності користувача з кібернетичною вразливістю інфраструктури, показуючи, що індекс вразливості v_i нелінійно зростає пропорційно добутку покриття та автономії ($s_i a_i$).

Цифровий суверенітет та безпека громадян в епоху автономізації державних сервісів залежать не від досконалості алгоритмів, а від наявності вбудованих структурних обмежень, які інженерно запобігають переходу інфраструктури від інструменту надання послуг до механізму необоротного домінування. Керована напруга між ефективністю, агентністю та стійкістю має стати новим архітектурним стандартом державного цифрового управління, де конфліктологія III регулюється не постфактум аудитами, а математично обґрунтованими межами фазового простору.

Список використаних джерел

1. An introduction to cybernetics. by: Ashby, William Ross. Publication date: 1956
2. Yeung, K., 2018. Algorithmic regulation: A critical interrogation. Regulation & governance, 12(4), pp. 05-523. DOI: 10.1111/rego.12158
3. Strogatz, S.H., 2001. Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering (studies in nonlinearity) (Vol. 1). Westview press.