Міністерство освіти і науки України

Державний заклад
«Південноукраїнський національний педагогічний
університет імені К. Д. Ушинського»
кафедра політичних наук і права
Центр соціально-політичних досліджень «Politicus»

X ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ З МІЖНАРОДНОЮ УЧАСТЮ

СУЧАСНА УКРАЇНСЬКА ДЕРЖАВА:

ВЕКТОРИ РОЗВИТКУ ТА ШЛЯХИ МОБІЛІЗАЦІЇ РЕСУРСІВ

30 квітня 2026 р.

м. Одеса

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ЗАКЛАД
«ПІВДЕННОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ПЕДАГОГІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ К. Д. УШИНСЬКОГО»
КАФЕДРА ПОЛІТИЧНИХ НАУК І ПРАВА
ЦЕНТР СОЦІАЛЬНО-ПОЛІТИЧНИХ ДОСЛІДЖЕНЬ «POLITICUS»

X ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ
з міжнародною участю

СУЧАСНА УКРАЇНСЬКА ДЕРЖАВА: ВЕКТОРИ РОЗВИТКУ ТА ШЛЯХИ МОБІЛІЗАЦІЇ РЕСУРСІВ

30 квітня 2026 року

м. Одеса

УДК 321(477)(063)
DOI: https://doi.org/10.24195/UkrainianState2026-10

Рекомендовано до друку Вченою радою Університету Ушинського
(протокол від 28 травня 2026 року № 14)

Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів : матеріали X Всеукраїнської науково-практичної конференції з міжнародною участю, м. Одеса, 30 квітня 2026 року. Одеса : ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2026. 583 с.

У збірнику матеріалів X Всеукраїнської науково-практичної конференції з міжнародною участю «Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів» представлено результати наукових досліджень науково-педагогічних працівників, здобувачів вищої освіти, молодих науковців та практиків із вітчизняних і зарубіжних закладів вищої освіти та наукових установ, об'єднаних прагненням до осмислення актуальних викликів державотворення, суспільного розвитку та післявоєнної відбудови України.

Матеріали збірника охоплюють широкий спектр актуальних проблем сучасної політичної, правової, економічної та соціогуманітарної науки. У наукових доповідях і дослідженнях висвітлено питання розвитку та модернізації політичних інститутів і процесів сучасної держави, правових та економічних механізмів відбудови України, інформаційної безпеки та протидії гібридним загрозам в умовах глобальних трансформацій. Значну увагу приділено філософським засадам державотворення, соціальним практикам і менеджменту соціокультурного розвитку, а також питанням євроінтеграції, транскордонної співпраці, міжнародних партнерств і регіональних стратегій сталого розвитку в умовах сучасних політичних та соціальних змін.

Збірник відображає високий рівень наукової дискусії та міждисциплінарного підходу до аналізу суспільно-політичних процесів, сприяє розвитку наукової комунікації та міжінституційної співпраці. Матеріали конференції становлять практичний і науковий інтерес для дослідників, викладачів, здобувачів освіти, представників органів державної влади, місцевого самоврядування та фахівців у сфері політичних, правових, економічних і соціогуманітарних наук.

Матеріали подано в авторській редакції. За зміст та достовірність наведених фактів, цитат і даних відповідальність несуть автори.

Кобус О. С.,
кандидатка фізико-математичних наук, доцентка
завідувачка КТЗК ЦКБ ННІ ІБ СК
НА СБ України
Бондаренко С. Ю.,
фахівець КТЗК ЦКБ ННІ ІБ СК
НА СБ України
член ГО «International educators and scholars foundation»
м. Київ, Україна

ЙМОВІРНІСНІ МОДЕЛІ ПРОГНОЗУВАННЯ ІНФОРМАЦІЙНИХ ІНЦИДЕНТІВ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Найбільш небезпечні інформаційні інциденти рідко починаються з очевидних сигналів, вони народжуються у статистичних відхиленнях, у слабких флуктуаціях даних, які на перший погляд не мають жодного значення. Саме в цих відхиленнях приховується передумова до майбутньої кризи, і завдання правоохоронних органів полягає не лише у реагуванні, а у випередженні таких процесів через використання складних ймовірнісних моделей прогнозування. У сучасному безпековому середовищі, де інформаційний простір є гібридним, багаторівневим і динамічно змінним, традиційні підходи до аналізу інцидентів виявляються недостатніми [2; 3]. Відтак виникає необхідність інтеграції математичних методів, зокрема ймовірнісного моделювання, у систему прийняття рішень правоохоронними структурами.

Ймовірнісні моделі прогнозування інформаційних інцидентів виступають інструментом формалізації невизначеності, що дозволяє кількісно оцінити ризики, виявити закономірності та сформувати обґрунтовані управлінські рішення. В умовах національної безпеки це набуває особливого значення, оскільки інформаційні інциденти можуть мати як локальний, так і стратегічний характер, впливаючи на стабільність державних інституцій, суспільну довіру та обороноздатність [1].

Першою моделлю, що заслуговує на детальний аналіз, є байєсівська ймовірнісна модель. В її основі лежить принцип оновлення ймовірностей на основі нової інформації. У контексті діяльності правоохоронних органів це означає, що кожен новий інформаційний сигнал, наприклад підозріла активність у мережі або аномалії у поведінці користувачів, змінює оцінку ризику виникнення інциденту. Сильна сторона цієї моделі полягає у її адаптивності та

здатності працювати в умовах неповної інформації. Вона дозволяє інтегрувати як статистичні дані, так і експертні оцінки, що особливо важливо у сфері національної безпеки, де значна частина інформації є закритою або неповною.

Водночас байєсівський підхід має суттєві обмеження. По-перше, він критично залежить від початкових апріорних ймовірностей, які часто формуються суб'єктивно. У правоохоронній практиці це може призводити до системних «перекосів» у оцінці загроз. По-друге, у складних багатовимірних системах обчислювальна складність байєсівських мереж різко зростає, що ускладнює їх практичне застосування в режимі реального часу. Крім того, класичні реалізації байєсівських моделей недостатньо враховують часову динаміку, що є критичним недоліком для прогнозування інформаційних атак, які розгортаються у часових ланцюгах.

Другою моделлю є марковські процеси, зокрема приховані марковські моделі. Вони базуються на припущенні, що майбутній стан системи залежить лише від її поточного стану. У сфері інформаційної безпеки це дозволяє моделювати послідовності подій, наприклад етапи кібератаки або ескалацію інформаційної операції. Приховані марковські моделі особливо ефективні для виявлення прихованих станів системи, які не спостерігаються безпосередньо, але впливають на видимі дані.

Перевагою цього підходу є його здатність працювати з часовими рядами та виявляти закономірності у динаміці подій. Це робить марковські моделі важливим інструментом для прогнозування розвитку інцидентів. Проте їх фундаментальне припущення про марковську властивість часто не відповідає реальності. У складних інформаційних системах історія подій може мати довготривалий вплив, який не обмежується лише попереднім станом. Таким чином, модель втрачає частину інформації, що може призводити до спрощення реальної картини загроз. Додатково варто зазначити, що калібрування таких моделей вимагає великих обсягів якісних даних, які у правоохоронній сфері не завжди доступні.

Третьою моделлю виступають пуассонівські процеси, які використовуються для моделювання рідкісних подій у часі. Інформаційні інциденти, особливо критичного рівня, часто мають саме такий характер, що робить цю модель привабливою для прогнозування. Пуассонівський підхід дозволяє оцінити інтенсивність виникнення подій та ймовірність їх появи у певному часовому інтервалі.

Сильна сторона цієї моделі полягає у її простоті та аналітичній прозорості. Вона добре підходить для первинної оцінки ризиків та побудови базових сценаріїв. Однак її застосування у сфері національної безпеки має суттєві

обмеження. По перше, вона передбачає незалежність подій, що у випадку інформаційних інцидентів є вкрай рідкісним явищем. Більшість атак є взаємопов'язаними та мають каскадний характер. По друге, модель не враховує змінності інтенсивності у часі, що є критичним недоліком в умовах гібридних загроз, де активність противника може різко зростати або спадати. Це обмежує її використання лише як допоміжного інструменту.

Четвертою моделлю є регресійні ймовірнісні моделі, зокрема логістична регресія. Вона дозволяє оцінити ймовірність настання інциденту залежно від набору факторів, таких як рівень кіберзахисту, інтенсивність інформаційних потоків, поведінкові характеристики користувачів. У правоохоронній діяльності це відкриває можливості для побудови систем раннього попередження.

Перевага логістичної регресії полягає у її інтерпретованості. Вона дозволяє чітко визначити, які фактори найбільше впливають на ризик інциденту. Це має важливе значення для управлінських рішень, оскільки дозволяє не лише прогнозувати, а й впливати на ситуацію. Проте ця модель також має обмеження. Вона передбачає лінійний зв'язок між змінними, що у складних інформаційних системах рідко відповідає дійсності. Крім того, вона чутлива до мультиколінеарності та якості вхідних даних, що може знижувати точність прогнозів.

Критичний аналіз існуючих ймовірнісних моделей свідчить про те, що жодна з них не є універсальною. Більшість підходів розроблялися для відносно стабільних систем, тоді як сучасне інформаційне середовище характеризується високою турбулентністю, гібридністю та адаптивністю загроз. Окремо варто підкреслити проблему переоцінки статистичних закономірностей. У практиці правоохоронних органів часто спостерігається тенденція до механічного перенесення математичних моделей без урахування контексту, що призводить до хибних висновків.

Додатковою проблемою є дефіцит якісних даних. Багато інформаційних інцидентів залишаються нерозкритими або не фіксуються належним чином, що формує викривлену статистичну базу. Це суттєво знижує ефективність будь яких ймовірнісних моделей. Крім того, існує проблема латентності загроз, коли значна частина активностей не проявляється у відкритих даних, що ускладнює їх моделювання.

У контексті забезпечення національної безпеки перспективним напрямом є інтеграція різних моделей у гібридні системи прогнозування. Поєднання байєсівських підходів з марковськими процесами, доповнене регресійним аналізом та методами машинного навчання, дозволяє частково компенсувати

недоліки кожної окремої моделі. Такий підхід забезпечує більш гнучке та адаптивне прогнозування, що відповідає сучасним викликам.

Водночас необхідно враховувати, що математичні моделі не можуть повністю замінити експертну оцінку. Ефективна система прогнозування повинна поєднувати кількісні методи з якісним аналізом, враховувати контекст, політичні та соціальні фактори, а також специфіку діяльності правоохоронних органів. Лише за таких умов можливо досягти високого рівня точності прогнозів та забезпечити своєчасне реагування на інформаційні загрози.

Отже, ймовірнісні моделі прогнозування інформаційних інцидентів є важливим інструментом у системі забезпечення національної безпеки, проте їх ефективність залежить від правильного вибору, адаптації та інтеграції у практичну діяльність. Критичне осмислення їх можливостей і обмежень дозволяє сформувати більш стійку та ефективну систему протидії інформаційним загрозам, що є ключовим завданням сучасних правоохоронних органів.

Література:

1. ENISA Threat Landscape 2024 : official report / European Union Agency for Cybersecurity. 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 26.04.2026).
2. Verizon 2024 Data Breach Investigations Report (DBIR). 17th ed. URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 26.04.2026).
3. Global Risks Report 2024 : report / World Economic Forum. 2024. URL: https://www.weforum.org/publications/global-risks-report-2024/ (дата звернення: 26.04.2026).

Ковалевська Л. В.,
магістр соціології
Харківський національний педагогічний
університет імені Г.С. Сковороди»
м. Івано-Франківськ, Україна

ТЕХНОЛОГІЇ ІНФОРМАЦІЙНОГО ВПЛИВУ НА СУСПІЛЬНУ СВІДОМІСТЬ У ПОЛІТИЧНИХ КОНФЛІКТАХ

Сучасні політичні конфлікти набули принципово нового виміру, в якому боротьба за суспільну свідомість є не менш вирішальною, ніж збройне

Наукове видання

Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів : матеріали X Всеукраїнської науково-практичної конференції з міжнародною участю, м. Одеса, 30 квітня 2026 року. Одеса : ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2026. 583 с.

Опубліковано в авторській редакції