

**Туровський Олександр**

доктор технічних наук, професор,

завідувач кафедри технічних систем кіберзахисту

Державний університет інформаційно-комунікаційних технологій, Київ, Україна

ORCID: 0000-0002-4961-0876

s19641011@ukr.net

ДИНАМІЧНА МОДЕЛЬ ОЦІНКИ СТАНУ КІБЕРЗАХИЩЕНОСТІ ДАНИХ У ГЕТЕРОГЕННІЙ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІЙ СИСТЕМІ

Анотація. В статті подано динамічну модель оцінки стану кіберзахищеності даних у гетерогенній інформаційно-комунікаційній системі. Сутність моделі полягає в динамічному оцінюванні стану кіберзахищеності даних шляхом послідовного оновлення ймовірностей станів взаємозалежних компонентів з урахуванням неповноти, достовірності та давності спостережень і подальшим обчисленням залишкового ризику. Її запропонована новизна полягає в узгодженому поєднанні типізованої структури станів, оцінювання якості доказів і повторного опрацювання затриманих спостережень за часом події, що розвиває можливості статичних незалежних оцінок та відомих динамічних байєсівських підходів. Залишковий ризик визначається як очікувані майбутні втрати, обчислені на основі оціненого спільного стану за заданих захисних дій. Запропоновано графову структуру, правила переходів, нормовану модель спостережень і алгоритм повторного фільтрування затриманих повідомлень. Проведено синтетичне оцінювання на 300 траєкторіях по 80 кроків для кожної конфігурації; побудовано шість рисунків і довірчі інтервали методом повторної вибірки траєкторій. За зростання частки пропусків від 0 до 60% показник Brier повної моделі змінювався від 0,0280 до 0,0555, статичної незалежної моделі — від 0,0664 до 0,0887. Досліджено затримки до п'яти кроків, якість доказів, помилкові залежності та вплив захисних дій. Установлено, що врахування неіснуючих залежностей може погіршувати результат. Отримані оцінки характеризують відтворюваний синтетичний тренд; вони не є валідацією на виробничій телеметрії. Розмежовано фізичний стан системи та невизначеність його оцінки, функціональні залежності й шляхи поширення компрометації, транспортну затримку та внутрішню давність доказу. Визначено умови нормування переходів і спостережень, монотонності впливу захисту та розрізнюваності станів. Практичне значення моделі полягає у підтримці порівняння заданих захисних дій за очікуваними наслідками для взаємозалежних компонентів. Подальші дослідження передбачають оцінювання параметрів за незалежною телеметрією та перевірку повної типізованої моделі.

Ключові слова: кіберзахищеність даних; динамічне оцінювання стану; динамічна байєсівська мережа; залишковий ризик; гетерогенна система; якість доказів; затримана телеметрія; калібрування.

ВСТУП

Постановка проблеми. Гетерогенна інформаційно-комунікаційна система об'єднує різноманітні апаратні та програмні компоненти, які забезпечують збирання, передавання, зберігання й оброблення даних, а також засоби їх кіберзахисту. До першої групи належать сенсори та інші пристрої Інтернету речей, робочі станції, сервери, мережеве обладнання, сховища й бази даних, прикладні програми та сервіси, що використовують ці дані. До другої - засоби керування доступом, міжмережеві екрани, системи виявлення вторгнень, контролю цілісності та моніторингу подій безпеки. Локальна оцінка кіберзахищеності окремого компонента вказаної мережі не завжди відображає наслідки для інших: компрометація сенсора може створити шлях несанкціонованого доступу до сервісу, порушення роботи сховища - зробити дані недоступними для прикладної програми, а надмірні повноваження облікового запису — розширити можливості поширення атаки. Значущість таких міжкомпонентних впливів і необхідність підтвердження дієвості захисних заходів обґрунтовано в попередніх роботах [1, 2].

Проблема полягає в тому, що фактичний стан цих компонентів змінюється в часі, тоді як відомості про нього надходять із різних джерел і не завжди є повними, достовірними та своєчасними. Зокрема,



журнали доступу, повідомлення засобів виявлення атак, результати перевірки конфігурацій і показники доступності сервісів відображають різні аспекти стану системи; відсутність повідомлення про загрозу сама по собі не підтверджує захищеність даних. Безперервний моніторинг має забезпечувати оцінювання дієвості захисту [3], а рішення щодо доступу — враховувати поточний контекст використання ресурсу [4]. Тому для розв'язання проблеми доцільно побудувати динамічну модель, яка поєднує опис станів даних, сервісів, мережеских вузлів, повноважень і засобів захисту; розмежовує функціональні залежності та можливі шляхи поширення компрометації; задає правила переходів між станами й оновлення їхніх імовірнісних оцінок за новими спостереженнями. Урахування якості доказів, часу події та затримки надходження повідомлень має забезпечити узгоджене використання неповної інформації, а обчислення залишкового ризику на основі оціненого спільного стану забезпечить підтримати порівняння захисних дій за очікуваними наслідками для даних.

Аналіз останніх досліджень і публікацій

В статті [1] розглядається вплив взаємодії лабораторних IoT-пристроїв із корпоративною мережею на кіберзахист, зокрема перекриття загроз і конвергенцію фізичної та інформаційної безпеки. Праця висвітлює подання зв'язків між сегментами. Для задачі цієї статті її принципову модель потрібно доповнити часовими станами, спостереженнями та формальним перерахунком імовірностей; безпосередньо переносити наведені там коефіцієнти як калібровані ймовірності не можна.

В роботі [2] подано методіку, що пов'язує аналіз ризику з вимогами, реалізацією захисту, доказами та рішенням про авторизацію. Методика містить аналітичні показники ризику, покриття вимог і повноти доказів. Її внесок важливий для відокремлення запланованого контролю від підтвердженого. Подальшої конкретизації для потокової телеметрії потребує зв'язок доказу з прихованим станом і правила врахування його давності.

Робота [5] присвячена оцінюванню конфігурацій мережі через граф атак і композицію впливів уразливостей. Це усуває частину недоліків незалежного аналізу вузлів: низькі локальні оцінки можуть утворювати небезпечний шлях. Однак метрика опору атаці та модель ймовірнісного стану даних мають різні семантики. Для нашої задачі додатково потрібні модель вимірювання й явне розмежування зв'язків функціонування та поширення компрометації.

В роботі [6] подано застосування динамічних байєсівських мереж для врахування часової зміни загроз, зокрема доступності експлойтів і виправлень. Отже, застосування динамічної байєсівської мережі саме по собі не становить новизни цієї статті. Додаткове питання тут — як узгоджено поєднати неоднорідні дані, дієвість контролю та спостереження з різними часом події і часом отримання.

В роботі [7] подано байєсівський підхід до оцінювання компрометації й вибору заходів посилення захисту з урахуванням ресурсних обмежень. Робота підтверджує корисність причинних залежностей для управління ризиком. Для поставленої нами задачі потрібна окрема перевірка того, як пропуски й затримки доказів змінюють калібрування поточної оцінки; задача оптимального розподілу бюджету в цій статті не розв'язується.

В статті [8] розглядається модель CEDRA, яка поєднує динамічну байєсівську мережу, відомості про загрози й уразливості з грошовими втратами для хмарного середовища. Тому зв'язок динамічних імовірностей з очікуваними втратами також має попередні результати. Наше уточнення стосується єдиного опису якості локальних доказів та їх прив'язування до часу події, а не першого запровадження фінансового чи залишкового ризику.

Робота [9] присвячена систематизації методів проєкції атак, прогнозування вторгнень і передбачення стану кібербезпеки. Поданий огляд важливий для розмежування задач: точність передбачення події ще не визначає калібрування ймовірності чи похибку очікуваних наслідків. Відповідно, у цій статті оцінювання стану, калібрування та похибка ризику перевіряються окремими показниками.

В роботі [10] подано застосування динамічних байєсівських мереж до кібератак на енергосистеми з поєднанням кроків атаки й аналітики виявлення. У ній порівняно точне й наближене виведення, зокрема за наявності доказів, і досліджено обчислювальні витрати. Цей результат спростовує припущення, ніби попередні динамічні моделі ігнорують спостереження. Наш акцент інший: втрата та несвоєчасність локальної телеметрії, її якість і наслідки помилково заданих залежностей.

В статті [11] розглядається байєсівське оновлення загроз на основі відомостей про кіберзагрози та відображення загроз на небезпечні стани конкретної системи. Це демонструє актуальність контекстного оновлення ризику. Розглянутий підхід орієнтований на інформацію про загрози й організаційне оцінювання; у нашій роботі одиницею оновлення є також локальний доказ про стан компонента, а залежності задаються явним графом.

Робота [12] присвячена обґрунтуванню наближеного виведення для складних стохастичних процесів із компактним поданням розподілу. Це створює шлях до масштабування, але наближення може змінити оцінку ризику. Тому демонстраційне дослідження нижче використовує точне виведення для



восьми спільних станів і не переносить його обчислювальні характеристики на великі корпоративні системи. Загальні засади динамічних мереж та байєсівського фільтрування викладено в [13, 14].

Основні невідповідності потребам задачі. Наведений цільовий огляд виявляє чотири вимоги, які потрібно перевіряти разом: розрізняти функціональну залежність і шлях компрометації; пов'язувати локальні докази з їх якістю та часом події; обчислювати ризик за спільним станом і підтвердженою дієвістю контролів; перевіряти не лише точність, а й калібрування та чутливість до помилок графа.

Виникає потреба у вирішенні нового актуального завдання, сутність якого полягає в тому, що компоненти мережі розглядаються на рівні їхніх станів, функціональних зв'язків і впливу на дані, без прив'язування до конкретного виробника або програмного продукту; окремо враховуються повноваження суб'єктів доступу та дієвість засобів захисту. Отже, предметом оцінювання є кіберзахищеність даних у процесі функціонування всієї системи, а не лише справність її захисних засобів.

Завдання по вирішенню вказаного завдання корелюється з запропонованими підходами до оцінки ризиків -. NIST SP 800-30 [15] та задає процес оцінювання ризику. А каталоги контролів стану кіберзахищеності [16] орієнтує тільки на зміст захисних заходів; Але конкретні ймовірності переходів і правила перерахунку мають бути визначені додатково. Що і обґрунтовує актуальність та необхідність вирішення визначено вище наукового завдання.

Мета статті: розробка динамічної моделі оцінки стану кіберзахищеності даних у гетерогенній інформаційно-комунікаційній системі, яка враховує залежності компонентів, зміну їхнього стану в часі, неповноту й затримки спостережень та якості доказів і забезпечує обчислення залишкового ризику на основі оціненого спільного стану за заданих захисних дій.

Межі застосовності моделі визначаються за точністю й калібруванням оцінок та чутливістю до помилкового завдання залежностей.

Мета конкретизується завданнями формалізації прихованого стану та переходів, побудови моделі спостережень і правил послідовного оновлення оцінки, перевірки розрізняюваності станів, обчислення похідного показника залишкового ризику та порівняння з контрольними моделями.

Науковий результат роботи буде полягати у розробці і формалізації динамічної моделі оцінки стану кіберзахищеності даних, яка поєднує залежності компонентів системи з правилами оновлення оцінок за неповними, різними за достовірністю та затриманими спостереженнями й забезпечує обчислення залишкового ризику як очікуваних втрат на заданому часовому горизонті. Байєсівський фільтр, граф атак і proper scoring rules використовуються в даній статті як відомі інструменти [5, 6, 7, 8, 13, 17].

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Структура системи та спостережувані величини

Під станом кіберзахищеності даних у цій роботі розуміємо стан збереження або порушення їх конфіденційності, цілісності та доступності в контексті залежних сервісів, повноважень і мережевих вузлів. Його оцінювання полягає в оновленні розподілу ймовірностей можливих станів за доступними спостереженнями. Дієвість засобів кіберзахисту є складовою спільного стану та чинником його переходів. Залишковий ризик є похідною величиною, яку обчислюють за оціненим розподілом, моделлю переходів і функцією втрат; він не ототожнюється зі станом даних.

Систему в дискретні моменти $t = 0, 1, \dots, T$ задаємо типізованим графом:

$$G = (V, E^f, E^a, E^c, \theta). \quad (1)$$

Множина V об'єднує дані V^D , сервіси V^S , суб'єктів із повноваженнями V^P , контроли V^C та мережеві вузли V^N . Ребра E^f задають функціональну залежність, E^a — можливість поширення компрометації, E^c — застосовність контролю; θ — параметри моделі. Ребро $u \rightarrow v$ у E^f означає потребу компонента v у функціонуванні u ; те саме ребро в E^a означає вплив компрометації u на ймовірність компрометації v . Ці відношення не ототожнюються [1, 5, 7].

Прихований фізичний стан має вигляд:

$$X_t = (D_t, S_t, P_t, C_t, N_t). \quad (2)$$

Стан даних $D_{i,t}$ описує конфіденційність, цілісність і доступність. Стани сервісів $S_{j,t}$, повноважень $P_{m,t}$, контролів $C_{k,t}$ та вузлів $N_{l,t}$ наведено в таблиці 1. Перелік контролів і об'єктів спостереження узгоджується з архітектурою системи, політикою доступу та відповідними групами заходів [4, 16].



Компоненти стану та доступні свідчення

Компонент	Множина станів або ознак	Приклади свідчень
Дані	Порушення або збереження конфіденційності, цілісності, доступності	Контроль цілісності; журнал доступу; тест відновлення
Сервіс	Працездатний; деградований; недоступний	Синтетичний запит; метрика затримки; журнал помилок
Повноваження	Відповідні політиці; надлишкові; скомпрометовані; заблоковані	Аудит прав; автентифікація; перевірка делегування
Контроль	Дієвий; ослаблений; обійдений; недоступний	Перевірка конфігурації; тест захисту; звіт агента
Вузол	Справний; скомпрометований; недоступний	Телеметрія виявлення; мережевий моніторинг

Фізичний стан «невідомо» не вводиться: невизначеність відображається розподілом знань про можливі стани. Позначимо через $\mathcal{Y}_t$ усі докази, отримані до часу t , включно з їх часом події. Оцінюваний стан знань визначається як $b_t(x) = P(X_t = x | \mathcal{Y}_t)$. Розподіл не є самим фізичним станом X_t [13, 14].

Переходи й прогноз стану

Модель переходів включає компрометацію, відновлення, зміну привілеїв і дієвості контролів. За заданої захисної дії u_t маємо:

$$T_\theta(x' | x, u_t, G) = P(X_{t+1} = x' | X_t = x, u_t, G, \theta). \quad (3)$$

Прогноз перед новими вимірюваннями задається стандартним кроком байєсівського фільтра [13, 14]:

$$b_{t+1}^-(x') = \sum_x T_\theta(x' | x, u_t, G) b_t(x). \quad (4)$$

Для двійкового індикатора компрометації $z_{v,t} \in \{0,1\}$ задаємо базову ймовірність несприятливого переходу та множник пригнічення окремо:

$$a_{v,t} = 1 - (1 - \mu_v)(1 - \rho_v z_{v,t}) \prod_{u \in \text{Pa}^a(v)} (1 - \beta_{uv} z_{u,t}). \quad (5)$$

$$h_{v,t} = a_{v,t} \prod_{k \in K(v)} (1 - \eta_{kv} e_{k,t}). \quad (6)$$

Тут $\mu_v \in [0,1]$ — базова ймовірність компрометації за крок; $\rho_v \in [0,1]$ — внесок збереження несприятливого стану; $\beta_{uv} \in [0,1]$ — сила залежності; $\text{Pa}^a(v)$ — батьківські вузли за графом атак; $K(v)$ — застосовні контролі; $\eta_{kv} \in [0,1]$ — ефективність контролю; $e_{k,t} \in [0,1]$ — його дієвість. За цих обмежень $0 \leq h_{v,t} \leq 1$. У (6) контроль зменшує ймовірність, оскільки $\partial h_{v,t} / \partial e_{k,t} \leq 0$. Дія включає запобігання та, коли це передбачено параметрами, усунення вже наявної компрометації. Для суто превентивного контролю множник має діяти лише на нові переходи, а відновлення задається окремо.

Формули (5)–(6) є обраною параметризацією типу noisy-OR із множником захисту; це не універсальний закон атак. Умовна незалежність наступних станів за повного попереднього стану є явним припущенням демонстраційної реалізації. Для спільної причини відмови слід додавати латентний вузол або спільний умовний розподіл [7, 13]. Контроль із невідомою дієвістю повинен залишатися випадковою складовою X_t , а не автоматично отримувати значення $e_{k,t} = 1$.

Функціональні залежності сервісів задаються окремими умовними розподілами:

$$P(S_{j,t+1} | S_{j,t}, D_t, N_t, P_t, C_t, u_t, G). \quad (7)$$

Наприклад, недоступність сервісу може бути наслідком недоступності залежного сховища без



компрометації самого сервісу. У (7) необхідно задавати правила резервування й деградації згідно з реальною архітектурою; граф атак не замінює цей опис.

Якість доказів і несвоєчасне надходження

Спостереження задаємо коротцем:

$$E_r = (y_r, v_r, \tau_r, a_r, s_r, c_r, q_r, \delta_r). \quad (8)$$

Позначення: y_r — значення, v_r — об'єкт, τ_r — час події, a_r — час отримання, s_r — джерело, $c_r \in [0,1]$ — повнота вмісту, $q_r \in [0,1]$ — надійність джерела, $\delta_r \geq 0$ — вік первинного свідчення на момент події. Наприклад, конфігураційний звіт може бути сформований сьогодні за застарілим аудитом. За визначеної швидкості втрати придатності $\lambda_r \geq 0$ використовуємо:

$$w_r = c_r q_r \exp(-\lambda_r \delta_r), 0 \leq w_r \leq 1. \quad (9)$$

Повнота c_r стосується змісту наявного повідомлення, а частка повністю відсутніх повідомлень задається окремо. Транспортна затримка $d_r = a_r - \tau_r$ відрізняється від віку первинного свідчення δ_r . Якщо достовірно відомі значення та час події, сам факт затримки не робить історичний вимір менш достовірним: його вплив на сучасний стан послаблюється переходами. Додаткове множення на експоненту транспортної затримки в цьому разі подвійно врахувало б час. Для справді застарілого або пошкодженого джерела застосовується (9); параметр визначається окремо за типом доказу [3, 14].

Правдоподібність спостереження є нормованою сумішшю:

$$\ell_r(x) = w_r P_0(y_r | X_{\tau_r} = x) + (1 - w_r) g_r(y_r). \quad (10)$$

Тут P_0 — модель інформативного джерела, g_r — розподіл неінформативного каналу, незалежний від стану. Для $w_r = 0$ свідчення не змінює відносних імовірностей станів; для $w_r = 1$ використовується повна модель джерела. Корельовані повідомлення не перемножуються як незалежні: потрібне групове правдоподіб'я або явна спільна причина. Це особливо важливо для дубльованих подій із різних систем збору.

Для своєчасного повідомлення оновлення має вигляд:

$$b_t(x) = \frac{\ell_t(x) b_t^-(x)}{\sum_{x'} \ell_t(x') b_t^-(x')}. \quad (11)$$

Затриманий доказ приєднується до історичного зрізу τ_r . Для всіх наявних на час t повідомлень цього зрізу обчислюємо $\ell_{\tau|t}(x)$; за їх відсутності покладемо $\ell_{\tau|t}(x) = 1$. Повторне фільтрування від контрольної точки до сучасного часу задається рекурсією:

$$\alpha_{k|t}(x) \propto \ell_{k|t}(x) \sum_{x'} T_\theta(x|x', u_{k-1}, G) \alpha_{k-1|t}(x'). \quad (12)$$

Кожний вектор у (12) нормується; фінально $b_t(x) = \alpha_{t|t}(x)$. Позначення $\alpha_{k|t}$ означає проміжне пряме повідомлення алгоритму з усіма отриманими доказами до зрізу k , а не згладжений розподіл історичного стану за всіма пізнішими спостереженнями. Архів має містити версії графа, переходів, дій і первинних доказів. Повторно обробляють усі збережені свідчення, але кожне враховують один раз [13, 14].

За пропуску виконується лише прогноз (4). Це означає відсутність нового негативного доказу, а не математичну гарантію незменшення ризику: за достатньої ймовірності відновлення прогнозований ризик може знижуватися. Якщо пропуски залежать від атаки, індикатор недоступності джерела потрібно включити до моделі спостережень. Експеримент нижче передбачає випадкові пропуски, незалежні від стану.

Залишковий ризик та умови коректності

На основі оціненого спільного стану визначаємо похідний показник залишкового ризику. Функція втрат $L(x) \geq 0$ задається для спільного стану без повторного зарахування одного наслідку різним сервісам. Підхід «імовірність — наслідок» узгоджується з оцінюванням ризику [15], а включення втрат у динамічні мережі має попередній приклад у CEDRA [8]. На горизонті H за плану дій u визначаємо:



$$R_t^H(u) = \sum_x b_t(x) E[\sum_{h=1}^H \gamma^{h-1} L(X_{t+h}) | X_t = x, G, u, \theta]. \quad (13)$$

Коефіцієнт $\gamma \in (0,1]$ задає вагу майбутніх втрат. У розрахунках використано $\gamma = 1$. За фіксованих параметрів і дій залишковий ризик відрізняється від сценарію без додаткового захисту:

$$\Delta R_t^H = R_t^H(u^0) - R_t^H(u^{\text{act}}). \quad (14)$$

Обидва сценарії стартують з однакового b_t , мають однаковий горизонт і функцію втрат. Порівняння характеризує наслідки заданого втручання, а не автоматично оптимальний захід. Дієвість контролю підтверджується його тестами, конфігураційними доказами та моніторингом [2, 3, 16].

Коректність вимагає невід'ємності й нормування переходів та емісій, єдиної часової основи, відсутності дублювання доказів і версіонування структури. Для (6) перевіряється монотонність щодо ефективності захисту. Окремо перевіряються допустимість повноважень і узгодженість функціональних залежностей із політикою доступу [4].

Потрібно розрізняти розрізняваність станів за відомих параметрів та ідентифікованість самих параметрів [18]. Нехай $O_{xy} = P(Y = y | X = x)$ — матриця емісій. Повний рядковий ранг O є достатньою умовою ін'єктивності відображення розподілу прихованих станів у розподіл спостережень. Він не означає безпомилкове визначення стану за одним випадковим повідомленням. Для трьох незалежних умовно на стані двійкових каналів із вагою $w = 0,9$ чутливість суміші дорівнює 0,815, частота хибних тривог — 0,05. Одновузлова матриця має ненульовий визначник, а повна матриця емісій — ранг 8. За відсутності всіх доказів інформативність зникає.

Параметри переходів і якості не оцінюються в цій роботі з реальних даних: їх задано для контрольованої перевірки. Наприклад, окремі значення c_r та q_r неможливо відновити лише з їх добутку без додаткових вимірювань. Відповідно, повний ранг емісій не доводить ідентифікованість усієї параметричної моделі; для цього потрібні часові серії, обмеження моделі та незалежна перевірка [14, 18].

МЕТОДИКА ДОСЛІДЖЕННЯ

Організація обчислювального дослідження

Демонстраційний стенд моделює ланцюг $A \rightarrow S \rightarrow D$: лабораторний IoT-вузол, залежний сервіс і набір даних. Це редукована реалізація підмоделі поширення компрометації, а не повна емпірична перевірка всіх станів (2). Три двійкові змінні утворюють вісім спільних станів; виведення точне. У кожній конфігурації згенеровано 300 незалежних траєкторій по 80 кроків. Початкове зерно генератора — 19092026; однакові потоки випадкових чисел забезпечують парне порівняння методів і кероване зіставлення умов. Початковий спільний розподіл — добуток бернуллівських розподілів із параметрами μ .

Таблиця 2

Параметри й варійовані умови синтетичного стенда

Показник	Значення
Базові ймовірності	$\mu = (0,01; 0,01; 0,005)$
Збереження стану	$\rho = (0,95; 0,90; 0,90)$
Номінальні залежності	$\beta_{AS} = 0,35, \beta_{SD} = 0,25$
Чутливість і специфічність інформативного каналу	0,90 та 0,95
Номінальна вага доказу	$w = 0,90$
Умовні неперекривні втрати	$L(z) = 10z_A + 80z_S + 100z_D$
Частка випадкових пропусків	0; 0,2; 0,4; 0,6
Максимальна затримка	0; 1; 3; 5 кроків
Вага доказу в аналізі якості	0,4; 0,6; 0,8; 1,0
Множник істинних залежностей	0; 0,5; 1,0; 1,5

Для неінформативного каналу ймовірність тривоги становить 0,05. Отже, за (10) маємо $P(Y = 1 | z = 1) = 0,05 + 0,85w$ та $P(Y = 1 | z = 0) = 0,05$. Генератор і оцінювач використовують однакові емісії; експеримент перевіряє властивості заданої моделі, а не навчання параметрів. Аналіз якості варіює сукупну



вагу w , а не намагається розрізнити ефекти повноти, надійності та внутрішньої давності, що дають однакову вагу.

Порівнювані методи. Статична незалежна модель використовує стаціонарні маргінальні ймовірності номінального процесу та останнє отримане вимірювання для кожного вузла, але не виконує часовий прогноз і не враховує спільні залежності. Це сильніший базовий варіант, ніж повторне використання малих базових ймовірностей на кожному кроці. Динамічна модель без залежностей застосовує той самий фільтр, але всі міжвузлові коефіцієнти поширення нульові. Повна динамічна модель використовує номінальний граф. Обидві динамічні моделі обробляють затримані докази за (12).

У базовій конфігурації частка пропусків дорівнює 0,2, затримка нульова, вага доказу — 0,9. В одній серії змінюється лише один фактор. Для максимальної затримки d_{max} кожне наявне повідомлення незалежно отримує затримку, рівномірну на цілих значеннях від нуля до d_{max} . Тому повідомлення можуть надходити поза чергою. Докази, які ще не отримані на поточний час, не використовуються; кінцеве «дозавантаження» після останнього кроку не виконується.

В аналізі помилки залежностей генератор використовує $\beta^{true} = s\beta$, а повна модель зберігає номінальне $s = 1$. Саме ця серія перевіряє наслідки невідповідності моделі істині. В інших серіях параметри генератора відомі оцінювачу. Порівняння з алгоритмами конкретних публікацій [6, 7, 8, 10, 11] не проводиться: наведені базові варіанти — власні контрольовані спрощення.

Для якості ймовірнісної оцінки застосовується двійковий показник Brier [17, 19]:

$$BS = \frac{1}{3NT} \sum_{i=1}^N \sum_{t=1}^T \sum_{v=1}^3 (p_{itv} - z_{itv})^2. \quad (15)$$

Тут $N = 300$, $T = 80$, p_{itv} — оцінена ймовірність, z_{itv} — відомий симуляційний стан. Brier характеризує загальну якість ймовірнісного прогнозу, а не лише калібрування. Калібрування додатково оцінюється reliability diagram і показником ECE за десятьма рівними інтервалами [20]:

$$ECE = \sum_{b=1}^{10} \frac{n_b}{3NT} |p_b - z_b|. \quad (16)$$

Порожні інтервали не враховуються. Показник залежить від групування й обсягу даних; мала ECE не доводить точності на будь-якому рівні ризику.

Нормована похибка одноетапного ризику порівнює оцінку з еталонним умовним очікуванням за відомого симуляційного стану:

$$MAE_R = \frac{1}{NT} \sum_{i,t} \left| \frac{R_{it}^1 - R_{it}^*}{190} \right|, R_{it}^* = E_{\theta^{true}}[L(X_{t+1})|X_t = x_{it}]. \quad (17)$$

Цей еталон використовує прихований стан лише для оцінювання, а не як вхід фільтра. Статична модель прогнозує незмінність поточної оцінки втрат. Показник (17) не тотожний похибці відносно одиничного реалізованого збитку, що містив би додаткову випадковість майбутнього переходу.

Довірчі інтервали 95% для середніх Brier і похибки ризику одержано процентильним bootstrap: 2000 вибірок із поверненням за цілими траєкторіями. Для різниці методів повторно вибирали парні траєкторії. Залежні часові кроки не вважаються незалежними спостереженнями. Інтервали характеризують варіацію синтетичних запусків за фіксованих параметрів, а не невизначеність самих параметрів чи графа.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Пропуски телеметрії

За збільшення пропусків від 0 до 60% Brier повної моделі зріс від 0,0280 до 0,0555, а статичної — від 0,0664 до 0,0887. Повна модель має нижчу похибку на кожному рівні, однак інформаційні втрати залишаються помітними (рис. 1). За 20% пропусків парна різниця Brier між повною моделлю та моделлю без залежностей становила -0,0096, 95% інтервал [-0,0109; -0,0083]. Від'ємний інтервал підтримує користь залежностей у цьому синтетичному сценарії.



Таблиця 3

Оцінювання за пропущеної телеметрії — середні та 95% довірчі інтервали

Пропуски	Модель	Brier та 95% інтервал	MAE ризику та 95% інтервал
0%	Статична	0,0664 [0,0632; 0,0699]	0,1217 [0,1185; 0,1249]
0%	Без залежностей	0,0355 [0,0328; 0,0385]	0,0717 [0,0665; 0,0766]
0%	Повна	0,0280 [0,0259; 0,0302]	0,0513 [0,0485; 0,0540]
20%	Статична	0,0707 [0,0671; 0,0745]	0,1263 [0,1227; 0,1298]
20%	Без залежностей	0,0442 [0,0407; 0,0479]	0,0839 [0,0781; 0,0897]
20%	Повна	0,0346 [0,0320; 0,0374]	0,0623 [0,0590; 0,0654]
40%	Статична	0,0788 [0,0746; 0,0830]	0,1347 [0,1306; 0,1386]
40%	Без залежностей	0,0561 [0,0518; 0,0608]	0,0999 [0,0930; 0,1066]
40%	Повна	0,0438 [0,0406; 0,0472]	0,0774 [0,0736; 0,0812]
60%	Статична	0,0887 [0,0838; 0,0938]	0,1451 [0,1402; 0,1498]
60%	Без залежностей	0,0713 [0,0657; 0,0771]	0,1204 [0,1123; 0,1282]
60%	Повна	0,0555 [0,0515; 0,0597]	0,0972 [0,0925; 0,1019]

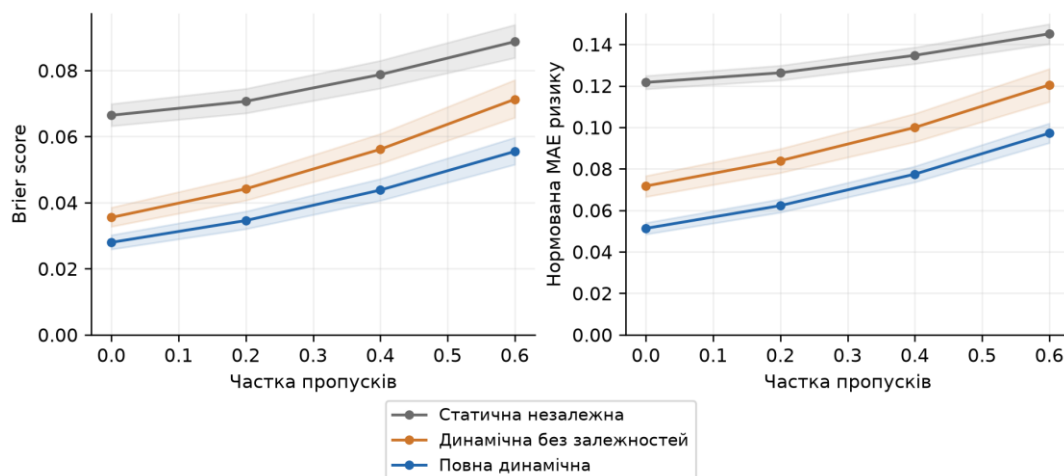


Рис. 1. Залежність Brier score та нормованої похибки ризику від частки пропусків. Затінені області — 95% bootstrap-інтервали середніх за траєкторіями; менше значення краще

Несвоєчасне надходження

Для повної моделі збільшення максимальної затримки від нуля до п'яти кроків змінило Brier з 0,0346 до 0,0624; нормована похибка ризику змінилася з 0,0623 до 0,1089. За максимальної затримки п'ять кроків Brier статичного варіанта дорівнював 0,0997 (рис. 2). Обробка за часом події не відновлює невимірний сучасний стан, але дозволяє узгоджено використовувати отриману історичну інформацію. Окремої абляції з навмисно неправильним часом події тут немає, тому ефект лише алгоритму повторної обробки не відділено від загального ефекту динамічної моделі.

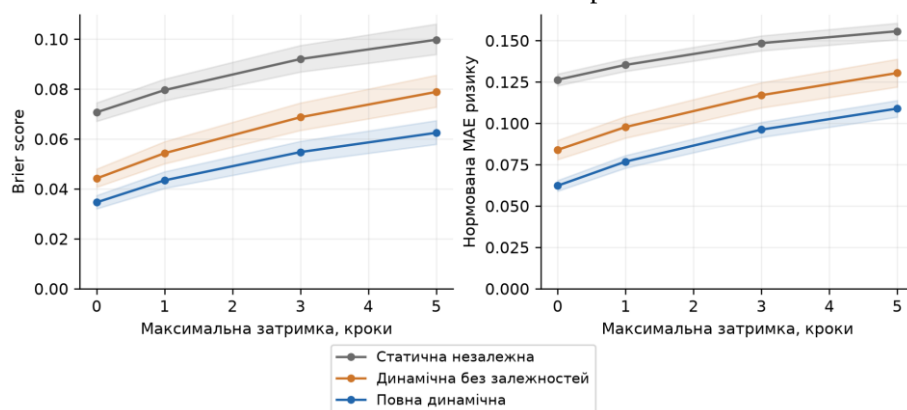


Рис. 2. Оцінювання за випадкової затримки від нуля до заданого максимуму. Частка пропусків — 20%, вага доказів — 0,9; часові позначки вважаються точними

Якість доказів і калібрування

За зростання ваги доказу від 0,4 до 1,0 Brier повної моделі зменшився з 0,0756 до 0,0276; нормована похибка ризику — з 0,1299 до 0,0511 (рис. 3). Це кількісно показує вплив якості спостережень за відомої моделі каналу. Калібрування ваги на незалежних даних цим дослідом не перевірено.

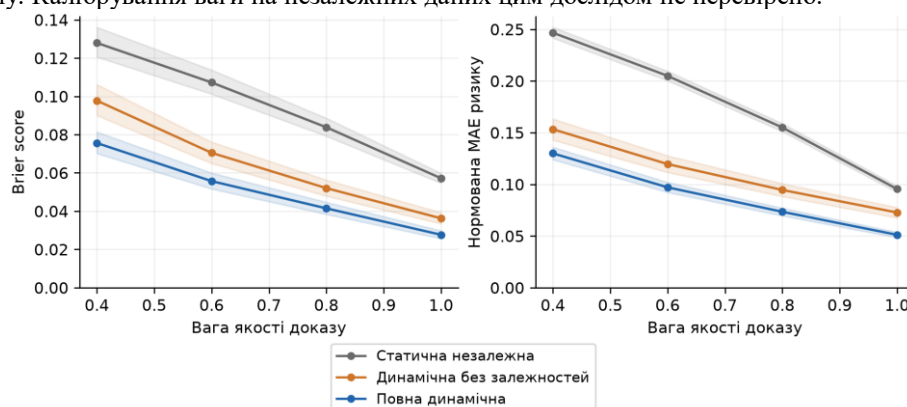


Рис. 3. Вплив ваги доказу на точність і похибку ризику за 20% пропусків без затримки. Генератор та оцінювач використовують однакову модель надійності

У базовому сценарії ESE становила 0,0014 для повної моделі, 0,0238 для моделі без залежностей і 0,0195 для статичного варіанта. На рисунку 4 наведені частоти за групами прогнозованої ймовірності. Оцінки на краях шкали можуть спиратися на меншу кількість прогнозів; для цих кривих окремі довірчі інтервали не обчислювалися.

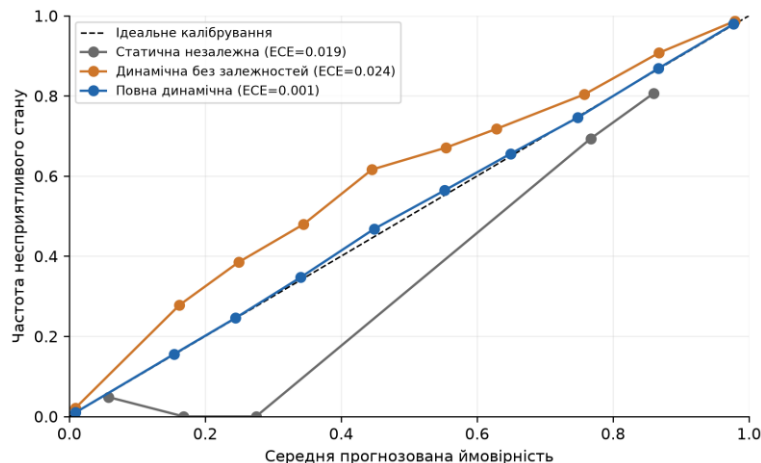


Рис. 4. Калібрування вузлових ймовірностей у базовій конфігурації. Пунктир відповідає рівності прогнозованої ймовірності та частоти стану; наведено ESE для десяти рівних інтервалів

Помилкове задання залежностей

За відсутності справжніх залежностей Брієр повної моделі дорівнював 0,0306, тоді як моделі без залежностей — 0,0233. За номінальних залежностей відповідні значення становили 0,0346 та 0,0442 (рис. 5). Таким чином, включення ребер не є безумовно корисним: неіснуючий шлях компрометації поширює помилкове припущення між вузлами. Результат визначає потребу перевіряти граф перед застосуванням оцінки до реальних даних.

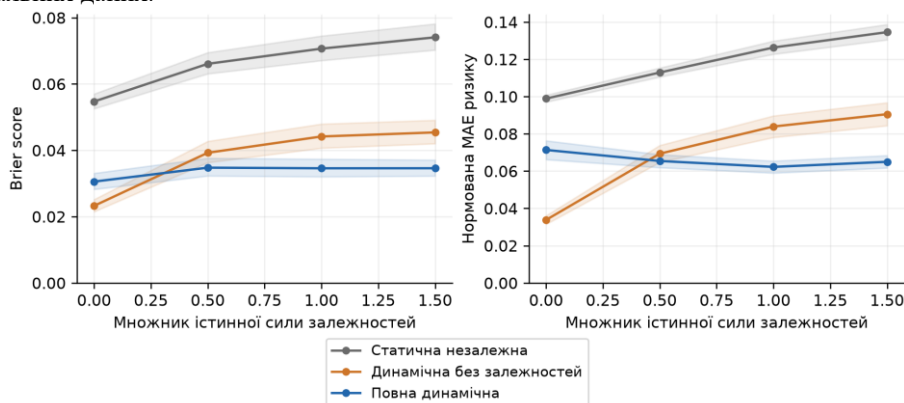


Рис. 5. Чутливість до істинної сили міжвузлових залежностей. Параметри повного оцінювача незмінні; значення нуль означає відсутність залежностей у генераторі

Оцінювання захисних дій

Окремий детермінований розрахунок демонструє застосовність функціонала (13). Вихідний розподіл утворено з початкового розподілу стелда після однієї тривоги на вузлі А за ваги $w = 0,9$; інші вузли не спостерігаються. Ефективний рівень пригнічення c змінюється від нуля до 0,9; для всіх вузлів у (6) використовується множник $1 - c$. Це умовний агрегований контроль, що поєднує запобігання та усунення компрометації; він не ідентифікується з конкретним виробом. Для кожного значення сили залежностей обчислено точне очікування на п'ять кроків та нормування:

$$\tilde{R}_t^5(c) = \frac{R_t^5(c)}{5 \cdot 190}. \quad (18)$$

За номінальних залежностей нормований п'ятикроковий ризик без додаткового пригнічення дорівнює 0,0883; за рівня 0,6 — 0,0110, за рівня 0,9 — 0,0017. Рисунок 6 показує також вплив слабших і сильніших залежностей. Усі криві монотонно спадають за посилення заданого контролю, що перевірено програмно. Вартість захисту та невизначеність його реальної дієвості до цього розрахунку не включені.

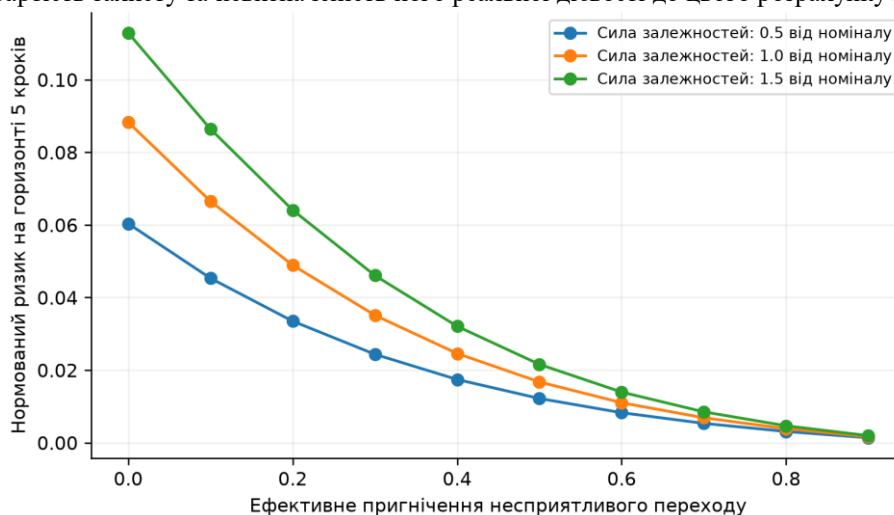


Рис. 6. Прогноз залишкового ризику для різної дієвості умовного захисту та різної сили залежностей. Криві — точні модельні очікування, а не середні вимірної ефективності засобів захисту

**Узагальнення результатів обчислювального дослідження**

По-перше, часова пам'ять і міжвузлові залежності покращують оцінювання в заданому каскадному сценарії: повна модель має нижчий Brier за два базові варіанти на всіх досліджених рівнях випадкових пропусків. Зіставлення з моделлю без залежностей відокремлює внесок ребер від внеску часової пам'яті.

По-друге, затримки й погіршення якості доказів збільшують похибку. Повторне фільтрування забезпечує коректне використання історичних вимірювань, але не усуває втрати інформації про сучасний стан. Тому результати підтримують вимогу зберігати часові позначки та підвищувати надійність каналів збору телеметрії.

По-третє, перевага залежить від адекватності графа: за відсутності справжніх ребер модель без залежностей точніша за повну номінальну модель. Перед використанням у практичній системі потрібні перевірка графа та окреме оцінювання невизначених коефіцієнтів.

По-четверте, модель дозволяє зіставляти задані захисні дії за очікуваними наслідками на однаковому горизонті. Монотонне зниження ризику на рисунку 6 підтверджує узгодженість параметризації контролю; це не емпіричний доказ ефективності конкретного засобу захисту. Для вибору заходу потрібні фактичні випробування, витрати й допустимі рівні ризику.

Обговорення та межі застосовності

Формалізація деталізує динамічне оцінювання стану кіберзахищеності даних за залежностей компонентів і неоднорідної якості доказів, мотивоване [1, 2], та використовує відомі засади байєсівського оцінювання [6, 7, 8, 13]. Її прикладна цінність полягає в узгодженому оновленні розподілу станів і використанні цього розподілу для обчислення залишкового ризику та порівняння заданих захисних дій. Порівняльний аналіз не дає підстав стверджувати абсолютну новизну всіх елементів окремо або перевагу над усіма опублікованими методами.

Стенд має лише три двійкові компоненти. Він не відтворює повний простір станів конфіденційності, цілісності, доступності, політик доступу та невідомої дієвості контролів. В основних серіях генератор узгоджений із фільтром; лише серія з різною силою ребер порушує це припущення. Не перевірено залежні від атаки пропуски, помилки часових позначок, корельовані джерела, невідому спільну причину, навчання параметрів або виробничу телеметрію. Надійність ваги доказу приймається відомою; її оцінювання є окремою задачею.

Точне виведення експоненційно залежить від кількості локальних змінних. Для більшого графа можливі факторизація або частинкове наближення [12, 14]; їх вплив на калібрування та ризик потрібно перевіряти окремо. Результати [10] демонструють важливість такого аналізу, але їх обчислювальні показники не переносяться на нашу реалізацію.

Для впровадження необхідно сформувати інвентар компонентів і залежностей; узгодити стани з політикою доступу; оцінити параметри переходів і сенсорів на окремих даних; встановити вікно зберігання доказів; визначити неперекривні категорії втрат. Після цього модель може підтримувати моніторинг і ранжування варіантів захисту в межах загального процесу управління ризиком [3, 4, 15, 16]. Автоматичні рішення про блокування доступу в цьому дослідженні не розробляються.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На підставі аналізу десяти попередніх праць і методичних джерел обґрунтовано постановку динамічного оцінювання стану кіберзахищеності даних за міжкомпонентних залежностей, неповних і затриманих спостережень. Залишковий ризик визначено як очікувані майбутні втрати на основі оціненого спільного стану за заданих захисних дій. Уточнено межі внеску відносно раніше розроблених графів атак, динамічних байєсівських мереж і моделей втрат.

Задано типізовану структуру стану, правила переходів, нормовану модель спостережень та алгоритм повторного фільтрування, що забезпечують послідовне оновлення оцінки за зміни стану компонентів у часі. Розмежовано стан кіберзахищеності даних, дієвість засобів кіберзахисту та невизначеність оцінки; транспортну затримку й давність первинного свідчення; розрізняваність станів та ідентифікованість параметрів. Параметризація захисту задовольняє умову незростання ймовірності несприятливого переходу за посилення дієвого контролю.

Синтетичні розрахунки з довірчими інтервалами демонструють можливість оцінювання пропусків, затримок, якості доказів, помилок залежностей та захисних дій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тарасенко, Я., Туровський, О., Іванкін, В., Матусяк, П., & Томашевський, М. (2025). Забезпечення кіберзахисту корпоративної мережі передачі даних в ході організації взаємодії між пристроями IoT



- дослідницьких лабораторій. *Вимірювальна та обчислювальна техніка в технологічних процесах*, 2(82), 334–343. <https://doi.org/10.31891/2219-9365-2025-82-48>
2. Іванченко, Є., Туровський, О., & Рижаков, М. (2026). Методика побудови системи безпеки об'єкта інформаційної діяльності для роботи з інформацією з обмеженим доступом. *Вимірювальна та обчислювальна техніка в технологічних процесах*, (3), 309–320. <https://doi.org/10.31891/2219-9365-2026-87-37>
 3. Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST SP 800-137). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-137>
 4. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST SP 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
 5. Wang, L., Singhal, A., & Jajodia, S. (2007). Measuring the overall security of network configurations using attack graphs. In *Data and Applications Security XXI* (pp. 98–112). Springer. https://doi.org/10.1007/978-3-540-73538-0_9
 6. Frigault, M., Wang, L., Singhal, A., & Jajodia, S. (2008). Measuring network security using dynamic Bayesian network. In *Proceedings of the 4th ACM Workshop on Quality of Protection* (pp. 23–30). ACM. <https://doi.org/10.1145/1456362.1456368>
 7. Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1), 61–74. <https://doi.org/10.1109/TDSC.2011.34>
 8. Behbehani, D., Komninos, N., Al-Begain, K., & Rajarajan, M. (2023). Cloud Enterprise Dynamic Risk Assessment (CEDRA): A dynamic risk assessment using dynamic Bayesian networks for cloud environment. *Journal of Cloud Computing*, 12, Article 79. <https://doi.org/10.1186/s13677-023-00454-2>
 9. Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2019). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, 21(1), 640–660. <https://doi.org/10.1109/COMST.2018.2871866>
 10. Cerotti, D., Savarero, D., Codetta Raiteri, D., Dondossola, G., Egidi, L., Franceschinis, G., Portinale, L., & Terruggia, R. (2025). Dynamic Bayesian networks for the detection and analysis of cyber attacks to power systems. *IEEE Access*, 13, 186289–186306. <https://doi.org/10.1109/ACCESS.2025.3624345>
 11. Thevaratnam, S., & Rezaeifar, Z. (2026). Quantifying cyber threat using Bayesian statistical analysis. *International Journal of Information Security*, 25, Article 43. <https://doi.org/10.1007/s10207-026-01220-6>
 12. Boyen, X., & Koller, D. (1998). Tractable inference for complex stochastic processes. In *Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence* (pp. 33–42). Morgan Kaufmann. <https://ai.stanford.edu/~xb/uai98/index.html>
 13. Murphy, K. P. (2002). *Dynamic Bayesian networks: Representation, inference and learning* [Doctoral dissertation, University of California, Berkeley]. <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2002/8174.html>
 14. Särkkä, S., & Svensson, L. (2023). *Bayesian filtering and smoothing* (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781108917407>
 15. National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST SP 800-30 Rev. 1). <https://doi.org/10.6028/NIST.SP.800-30r1>
 16. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). <https://doi.org/10.6028/NIST.SP.800-53r5>
 17. Gneiting, T., & Raftery, A. E. (2007). Strictly proper scoring rules, prediction, and estimation. *Journal of the American Statistical Association*, 102(477), 359–378. <https://doi.org/10.1198/016214506000001437>
 18. Allman, E. S., Matias, C., & Rhodes, J. A. (2009). Identifiability of parameters in latent structure models with many observed variables. *The Annals of Statistics*, 37(6A), 3099–3132. <https://doi.org/10.1214/09-AOS689>
 19. Brier, G. W. (1950). Verification of forecasts expressed in terms of probability. *Monthly Weather Review*, 78(1), 1–3. [https://doi.org/10.1175/1520-0493\(1950\)078<0001:VOFEIT>2.0.CO;2](https://doi.org/10.1175/1520-0493(1950)078<0001:VOFEIT>2.0.CO;2)
 20. Guo, C., Pleiss, G., Sun, Y., & Weinberger, K. Q. (2017). On calibration of modern neural networks. In *Proceedings of the 34th International Conference on Machine Learning* (Vol. 70, pp. 1321–1330). PMLR. <https://proceedings.mlr.press/v70/guo17a.html>

**Oleksandr Turovsky**

Doctor of Technical Sciences, Professor,

Head of the Department of Technical Cybersecurity Systems

State University of Information and Communication Technologies, Kyiv, Ukraine

ORCID: 0000-0002-4961-0876

s19641011@ukr.net

DYNAMIC MODEL FOR ASSESSING THE CYBERSECURITY STATE OF DATA IN A HETEROGENEOUS INFORMATION AND COMMUNICATION SYSTEM

Abstract. This study develops and evaluates a dynamic model for assessing the cybersecurity state of data in a heterogeneous information and communication system under incomplete and delayed observations, accounting for component dependencies and changes over time. Residual risk is derived from the estimated joint state as expected future loss under specified protective actions. The literature review recognises existing dynamic Bayesian approaches; the proposed contribution is a specific integration of typed states, evidence quality, event-time updates and a testable loss functional. A normalised observation model and an archive-based refiltering procedure are specified. Synthetic evaluation uses 300 trajectories of 80 steps per configuration, paired comparisons and trajectory-bootstrap confidence intervals. As missing observations increase from zero to 60%, the full model's Brier score rises from 0.0280 to 0.0555, compared with 0.0664 to 0.0887 for an independent static baseline. Six figures show sensitivity to missingness, delays of up to five steps, evidence quality, dependency misspecification and protective controls. Incorrectly assumed dependencies can degrade estimation relative to a model without dependencies. These findings establish behaviour on the stated synthetic benchmark, not validation on operational telemetry. The model distinguishes physical system states from uncertainty about these states, functional service dependencies from compromise propagation, and transport delay from the intrinsic age of evidence. Missing observations trigger prediction without introducing unsupported evidence of safety. Delayed observations are incorporated at their event time and the filter is rerun to the present using archived evidence and model versions. Conditions for normalised transitions and observations, monotonic protection effects and state distinguishability are specified. Residual risk is evaluated as expected future loss under a fixed protection scenario without claiming an optimal response policy. The practical value lies in comparing specified protective actions for interdependent components. The experiment covers a reduced three-component model; parameter learning, attack-dependent missingness, correlated sources and validation of the complete typed state remain subjects for further research.

Keywords: data cybersecurity; dynamic state estimation; dynamic Bayesian network; residual risk; heterogeneous system; evidence quality; delayed telemetry; calibration.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Tarasenko, Ya., Turovskiy, O., Ivankin, V., Matusiak, P., & Tomashevskiy, M. (2025). Zabezpechennia kiberzakhystu korporatyvnoi merezhi peredachi danykh v khodi orhanizatsii vzaємodii mizh prystroiamy IoT doslidnytskykh laboratorii [Ensuring cybersecurity of a corporate data transmission network during interaction between IoT devices in research laboratories]. *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh*, 2(82), 334–343. <https://doi.org/10.31891/2219-9365-2025-82-48>
2. Ivanchenko, Ye., Turovskiy, O., & Ryzhakov, M. (2026). Metodyka pobudovy systemy bezpeky obiekta informatsiinoi diialnosti dlia roboty z informatsiieiu z obmezhenym dostupom [Methodology for developing the security system of an information activity facility handling restricted-access information]. *Vymiriuvalna ta obchysliuvalna tekhnika v tekhnolohichnykh protsesakh*, (3), 309–320. <https://doi.org/10.31891/2219-9365-2026-87-37>
3. Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., Orebaugh, A., Scholl, M., & Stine, K. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST SP 800-137). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-137>
4. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST SP 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
5. Wang, L., Singhal, A., & Jajodia, S. (2007). Measuring the overall security of network configurations using



- attack graphs. In *Data and Applications Security XXI* (pp. 98–112). Springer. https://doi.org/10.1007/978-3-540-73538-0_9
6. Frigault, M., Wang, L., Singhal, A., & Jajodia, S. (2008). Measuring network security using dynamic Bayesian network. In *Proceedings of the 4th ACM Workshop on Quality of Protection* (pp. 23–30). ACM. <https://doi.org/10.1145/1456362.1456368>
 7. Poolsappasit, N., Dewri, R., & Ray, I. (2012). Dynamic security risk management using Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, 9(1), 61–74. <https://doi.org/10.1109/TDSC.2011.34>
 8. Behbehani, D., Komninos, N., Al-Begain, K., & Rajarajan, M. (2023). Cloud Enterprise Dynamic Risk Assessment (CEDRA): A dynamic risk assessment using dynamic Bayesian networks for cloud environment. *Journal of Cloud Computing*, 12, Article 79. <https://doi.org/10.1186/s13677-023-00454-2>
 9. Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2019). Survey of attack projection, prediction, and forecasting in cyber security. *IEEE Communications Surveys & Tutorials*, 21(1), 640–660. <https://doi.org/10.1109/COMST.2018.2871866>
 10. Cerotti, D., Savarro, D., Codetta Raiteri, D., Dondossola, G., Egidi, L., Franceschinis, G., Portinale, L., & Terruggia, R. (2025). Dynamic Bayesian networks for the detection and analysis of cyber attacks to power systems. *IEEE Access*, 13, 186289–186306. <https://doi.org/10.1109/ACCESS.2025.3624345>
 11. Thevaratnam, S., & Rezaeifar, Z. (2026). Quantifying cyber threat using Bayesian statistical analysis. *International Journal of Information Security*, 25, Article 43. <https://doi.org/10.1007/s10207-026-01220-6>
 12. Boyen, X., & Koller, D. (1998). Tractable inference for complex stochastic processes. In *Proceedings of the Fourteenth Conference on Uncertainty in Artificial Intelligence* (pp. 33–42). Morgan Kaufmann. <https://ai.stanford.edu/~xb/uai98/index.html>
 13. Murphy, K. P. (2002). *Dynamic Bayesian networks: Representation, inference and learning* [Doctoral dissertation, University of California, Berkeley]. <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2002/8174.html>
 14. Särkkä, S., & Svensson, L. (2023). *Bayesian filtering and smoothing* (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781108917407>
 15. National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments* (NIST SP 800-30 Rev. 1). <https://doi.org/10.6028/NIST.SP.800-30r1>
 16. National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). <https://doi.org/10.6028/NIST.SP.800-53r5>
 17. Gneiting, T., & Raftery, A. E. (2007). Strictly proper scoring rules, prediction, and estimation. *Journal of the American Statistical Association*, 102(477), 359–378. <https://doi.org/10.1198/016214506000001437>
 18. Allman, E. S., Matias, C., & Rhodes, J. A. (2009). Identifiability of parameters in latent structure models with many observed variables. *The Annals of Statistics*, 37(6A), 3099–3132. <https://doi.org/10.1214/09-AOS689>
 19. Brier, G. W. (1950). Verification of forecasts expressed in terms of probability. *Monthly Weather Review*, 78(1), 1–3. [https://doi.org/10.1175/1520-0493\(1950\)078<0001:VOFEIT>2.0.CO;2](https://doi.org/10.1175/1520-0493(1950)078<0001:VOFEIT>2.0.CO;2)
 20. Guo, C., Pleiss, G., Sun, Y., & Weinberger, K. Q. (2017). On calibration of modern neural networks. In *Proceedings of the 34th International Conference on Machine Learning* (Vol. 70, pp. 1321–1330). PMLR. <https://proceedings.mlr.press/v70/guo17a.html>

Отримано редакцією журналу / Received: 02.08.26

Прорецензовано / Revised: 24.08.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.