DOI: 10.35681/1560-9189.2025.27.2.345612

УДК 004.056

Д. В. Ланде[1], Ю. Б. Цирульнєв[2]
[1]Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна
[2]Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Проспект Берестейський, 37, 03056 Київ, Україна

Резильєнтність електронних архівів

Розглянуто сутність понять «резильєнтність» і «виживаність» інформаційних систем, проведено їхній порівняльний аналіз та уточнено застосовність до електронних архівів. Запропоновано підхід до оцінки резильєнтності електронних архівів як інформаційно-аналітичних систем обробки даних. Подано математичну формалізацію впливу кіберзагроз на функції електронних архівів і розглянуто модель адаптивної резильєнтності. На підставі визначень резильєнтності інформаційних систем згідно міжнародних стандартів і наукових досліджень введено та формалізовано критерій резильєнтного перерізу (Resilience Threshold Function) і функцію відновлення (Recovery Function). Введено поняття «резильєнтна інфраструктура електронного архіву» і окреслено можливості побудови профілю відновлення. Отримані результати створюють підґрунтя для вимірювання та підвищення рівня резильєнтності електронних архівів у процесах зберігання та використання електронних інформаційних ресурсів.

Ключові слова: *електронний архів, резильєнтність, критерій резільєнтного перерізу, функція резильєнтного відновлення, резильєнтна інфраструктура, адаптивна резильєнтність, динамічна резильєнтність.*

Вступ

Резильєнтність (resilience) — це здатність інформаційних систем адаптуватися, реагувати на кіберзагрози та відновлювати цілісність і функціональність після кіберінцидентів і кіберзагроз, техногенних катастроф, надзвичайних ситуацій, чи воєнних дій [1, 2]. На відміну від живучості (survivability) — здатності системи адаптуватися до нових непередбачуваних умов функціонування, протистояння небажаним впливам при реалізації основної функції [3], яка раніше розглядалася як здатність критичних систем підтримувати роботу після атак [6], резильєнтність означає відновлення системою повного спектра своїх функцій після інциденту та подальшу роботу в штатному режимі. Критерій резильєнтності можна визначити як відновлен-

ня рівня функціональності електронного архіву до початкового стану $F_{DA}(t) \to F_{DA}^0$ протягом скінченного часу після впливу кіберзагрози. Тобто, система є резильєнтною, якщо для будь-якої кібератаки T_i існує момент часу t_r, такий що: $F_{DA}(t_r) = F_{DA}^0$, де $F_{DA}(t)$ — функціональність архіву в момент часу t, а F_{DA}^0 — номінальний рівень функціональності. Подібні формальні підходи до визначення survivability інформаційних систем розроблялися ще у працях Knight, Strunk та Sullivan [5]. У контексті електронних архівів резильєнтність виступає критичною характеристикою, яка забезпечує сталість функціонування при зростаючих загрозах інформаційній безпеці. Разом з тим, питання формалізації резильєнтності електронних архівів і її відмінностей від виживаності залишаються відкритими. Метою статті є математична формалізація резильєнтності електронних архівів як інформаційно-аналітичних систем обробки даних і розроблення підходів до оцінки резильєнтності. Резильєнтність є критичною властивістю сучасних електронних архівів (Digital Archives, DA) — інформаційних системах класу Enterprise Content Management (ECM) і Content Service Platform (CSP) [4]. Забезпечення резильєнтності є необхідною умовою кібербезпеки. Частково цю тематику було розглянуто в роботі [7].

Кібервразливі функції електронних архівів

Дослідження проводилося на масиві кібервразливих функцій $F_{DA} = \{F_{DA_1}, F_{DA_2}, \ldots, F_{DA_{10}}\}$ систем класу ECM/CSP, де F_{DA_i} — функція електронного архіву, що зазначена в табл. 1.

Таблиця 1. Функції ECM/CSP-систем

Позначення	Функція	Опис
F_{DA_1}	Захоплення (Capture)	Автоматизоване перетворення фізичних і цифрових джерел інформації у внутрішні об’єкти архіву
F_{DA_2}	Індексування (Indexing)	Присвоєння структурованих і семантичних ключів пошуку документам для забезпечення їхньої ідентифікації і навігації
F_{DA_3}	Управління метаданими (Metadata Management)	Зберігання та обслуговування метаданих, пов’язаних з документами, що описують їхній контекст, походження і атрибути
F_{DA_4}	Пошук і доступ (Search & Retrieval)	Здійснення запитів до архіву та повернення релевантних документів на основі індексів та запитів користувача
F_{DA_5}	Контроль доступу (Access Control)	Керування правами доступу до документів відповідно до політик безпеки та ідентичності користувачів
F_{DA_6}	Утримання і знищення (Retention & Disposition)	Визначення строків зберігання, автоматичне видалення або архівація документів відповідно до політик
F_{DA_7}	Управління версіями (Version Control)	Фіксація та контроль усіх змін у документах із збереженням історії та можливістю відновлення

F_{DA_8}	Керування процесами (Workflow Management)	Моделювання і реалізація послідовностей дій користувачів і системи над документами у вигляді бізнес-процесів
F_{DA_9}	Аудит і логування (Audit & Logging)	Фіксація дій користувачів та змін у документах з метою аналізу, відповідності та безпеки
$F_{DA_{10}}$	Перевірка цілісності (Data Integrity Verification)	Перевірка достовірності вмісту архівних об'єктів за допомогою хеш-функцій або цифрових підписів

Кіберзагрози функціям електронних архівів

У межах цієї роботи досліджено підлягали кіберзагрози $FT_{DA} = \{FT_{DA_1}, FT_{DA_2}, \ldots, FT_{DA_{10}}\}$ функціям F_{DA} систем класу ECM/CSP, де FT_{DA_j} — кіберзагроза функції електронного архіву F_{DA_i}, що зазначена в табл. 2.

Таблиця 2. Кіберзагрози функціям ECM/CSP-системи

Позначення	Загроза	Опис
FT_{DA_1}	Несанкціонований доступ	Доступ до документів або систем без відповідного дозволу чи автентифікації
FT_{DA_2}	Порушення цілісності даних	Модифікація, знищення або пошкодження архівних даних без належного контролю
FT_{DA_3}	Перехоплення даних при передачі	Отримання вмісту архіву при його передачі через незахищені канали
FT_{DA_4}	Підробка метаданих	Несанкціоноване редагування або підміна метаданих для фальсифікації контексту або атрибуції
FT_{DA_5}	Атаки на AI/ML	Експлуатація вразливостей у моделей машинного навчання, які використовуються в архіві (наприклад, класифікаторів)
FT_{DA_6}	Маніпуляція даними:	Цілеспрямована зміна вмісту архіву для досягнення неправомірних цілей або впливу на аналітику
FT_{DA_7}	Prompt Injection	Введення зловмисних запитів у AI-моделі, що впливають на генерацію відповідей і класифікацію
FT_{DA_8}	Викрадення даних	Масове або приховане копіювання архівної інформації без дозволу та реєстрації
FT_{DA_9}	Дезінформація	Внесення неправдивих даних в архів з метою деструктивного впливу на подальший аналіз або прийняття рішень
$FT_{DA_{10}}$	Підробка цифрових підписів	Генерація фальшивих або підроблених електронних підписів, які проходять валідацію

Протидії кіберзагрозам функціям електронних архівів

У межах дослідження, запропоновано наступні заходи протидії $FTM_{DA} = \{FTM_{DA_1}, FTM_{DA_2}, \ldots, FTM_{DA_{10}}\}$, кіберзагрозам FT_{DA} функціям F_{DA} систем класу ECM/CSP, де FTM_{DA_k} — протидія загрозі FT_{DA_j} функції електронного архіву F_{DA_i}, що наведена в табл. 3.

Таблиця 3. Протидії кіберзагрозам функціям електронних архівів

Позначення	Протидія	Опис
FTM_{DA_1}	Шифрування	Перетворення даних у формат, непридатний до прочитання без криптографічного ключа
FTM_{DA_2}	Багатофакторна аутентифікація	Використання комбінації кількох факторів (пароль, біометрія, токен) для перевірки особи користувача
FTM_{DA_3}	Моніторинг активності	Безперервне відстеження та аналіз дій користувачів і систем для виявлення підозрілих аномалій
FTM_{DA_4}	Резервування та оновлення	Регулярне створення копій даних і підтримка їхньої актуальності для відновлення після інцидентів
FTM_{DA_5}	Верифікація та фільтрація запитів	Перевірка відповідності та безпечності вхідних запитів, особливо до AI/LLM модулів
FTM_{DA_6}	Виявлення аномалій	Використання моделей поведінки та машинного навчання для виявлення відхилень від нормальних патернів.
FTM_{DA_7}	Захист AI/ML	Укріплення моделей машинного навчання до атак типу adversarial input або data poisoning.
FTM_{DA_8}	Контроль доступу і логування	Накладання прав доступу і ведення журналів активності з подальшим аудитом.
FTM_{DA_9}	Перевірка цифрових підписів	Валідація цифрового підпису документа на основі відкритих сертифікатів або хешів.
$FTM_{DA_{10}}$	Захист метаданих	Використання криптографічного хешування та перевірки контрольних сум для збереження достовір-ності метаданих

Вплив кіберзагроз на функції електронного архіву

Вплив кіберзагроз на функції електронного архіву представлений у вигляді матриці, що надана в табл. 4 і у вигляді Графа 1 (рис. 1).

Таблиця 4. Вплив кіберзагроз на функції електронного архіву

	F_{DA_1}	F_{DA_2}	F_{DA_3}	F_{DA_4}	F_{DA_5}	F_{DA_6}	F_{DA_7}	F_{DA_8}	F_{DA_9}	$F_{DA_{10}}$
FT_{DA_1}	1	1	0	0	1	0	0	0	0	0
FT_{DA_2}	0	1	1	0	0	0	1	0	0	1
FT_{DA_3}	1	0	0	1	0	0	0	0	0	0
FT_{DA_4}	0	0	1	0	0	0	0	0	0	1
FT_{DA_5}	0	1	0	0	0	1	0	1	0	0
FT_{DA_6}	0	1	0	0	0	1	1	0	0	0
FT_{DA_7}	0	0	0	1	0	0	0	1	0	0
FT_{DA_8}	1	0	0	0	0	0	0	0	1	0
FT_{DA_9}	0	0	0	1	0	0	0	0	0	0
$FT_{DA_{10}}$	0	0	0	0	0	0	1	0	0	1

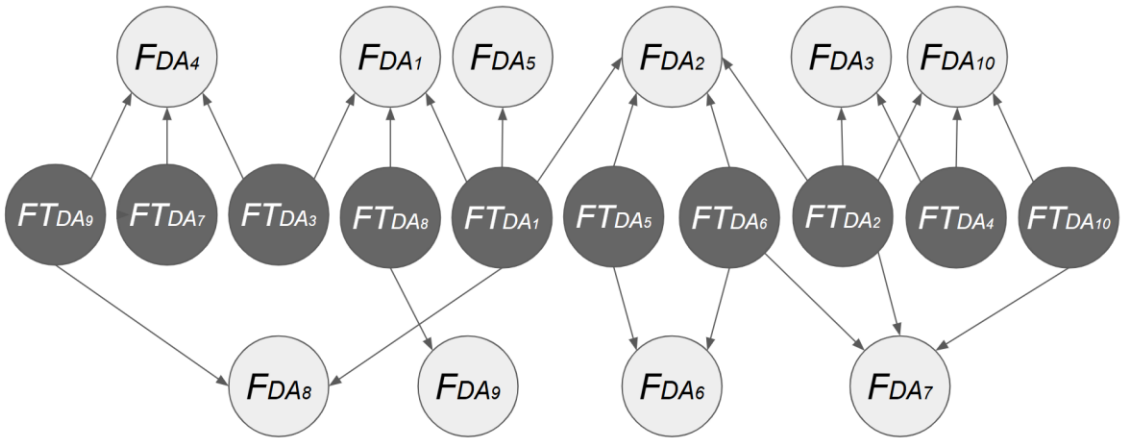

Рис. 1. Граф 1 — вплив кіберзагроз на функції електронного архіву

Протидія кіберзагрозам функціям електронного архіву

Запропоновано застосування заходів протидій кіберзагрозам, яке представлено у вигляді матриці, що надана в табл. 5 і у вигляді Графа 2 (рис. 2).

Таблиця 5. Протидії кіберзагрозам функціям електронного архіву

	FT_{DA_1}	FT_{DA_2}	FT_{DA_3}	FT_{DA_4}	FT_{DA_5}	FT_{DA_6}	FT_{DA_7}	FT_{DA_8}	FT_{DA_9}	$FT_{DA_{10}}$
FTM_{DA_1}	1	0	1	0	0	0	0	1	0	0
FTM_{DA_2}	1	0	0	0	0	0	0	0	0	0
FTM_{DA_3}	1	0	0	0	0	1	0	1	0	0
FTM_{DA_4}	0	1	0	0	0	0	0	0	0	1
FTM_{DA_5}	0	0	0	0	1	0	1	0	1	0
FTM_{DA_6}	0	0	0	0	0	1	0	0	1	0
FTM_{DA_7}	0	0	0	0	1	0	0	0	0	0
FTM_{DA_8}	1	0	0	0	0	0	0	1	0	0
FTM_{DA_9}	0	0	0	0	0	0	0	0	0	1
$FTM_{DA_{10}}$	0	0	0	1	0	0	0	0	0	0

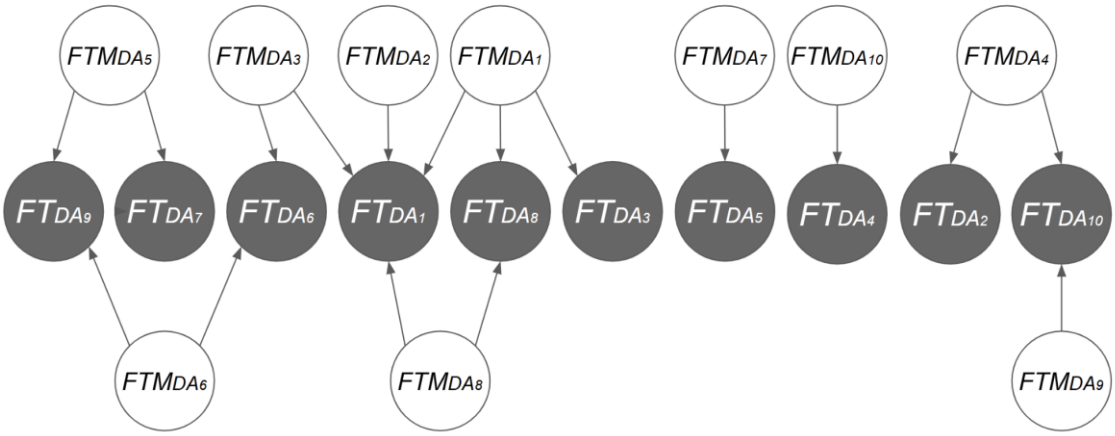

Рис. 2. Граф 2 — протидії кіберзагрозам функціям електронного архіву

Захист функцій електронного архіву

Захист функцій електронного архіву від впливу кіберзагроз шляхом застосуванням протидій кіберзагрозам представлено у вигляді матриці, що надана в табл. 6 і у вигляді Графа 3 (рис. 3).

Таблиця 6. Захист функцій електронного архіву

	F_{DA_1}	F_{DA_2}	F_{DA_3}	F_{DA_4}	F_{DA_5}	F_{DA_6}	F_{DA_7}	F_{DA_8}	F_{DA_9}	$F_{DA_{10}}$
FTM_{DA_1}	1	0	1	0	0	0	0	0	0	1
FTM_{DA_2}	0	0	0	0	1	0	0	0	0	0
FTM_{DA_3}	1	0	0	0	0	0	1	0	1	0
FTM_{DA_4}	0	0	0	0	0	1	1	0	0	1
FTM_{DA_5}	0	0	0	1	0	0	0	1	0	0
FTM_{DA_6}	0	0	0	0	0	1	1	0	0	0
FTM_{DA_7}	0	1	0	0	0	1	0	0	0	0
FTM_{DA_8}	0	0	0	0	1	0	0	0	1	0
FTM_{DA_9}	0	0	0	0	0	0	1	0	0	1
$FTM_{DA_{10}}$	0	0	1	0	0	0	0	0	0	0

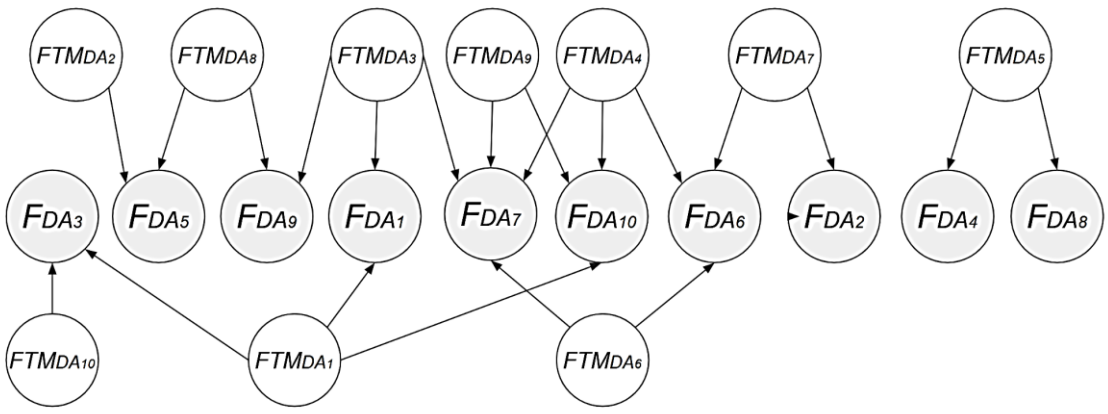

Рис 3. Граф 3 — захист функцій електронного архіву

Резильєнтність R_{DA} електронного архіву *DA* в умовах впливу кіберзагроз *FT* (Function Threat) $FT_{DA} = \{FT_{DA_1}, \dots FT_{DA_n}\}$ залежить від таких властивостей електронного архіву: A_{DA} — здатності *DA* передбачати вплив кіберзагрози; W_{DA} — здатності *DA* витримувати вплив кіберзагроз; Rc_{DA} — здатності *DA* відновлюватися після впливу кіберзагроз; Ad_{DA} — здатності адаптуватися до впливу кіберзагроз:

$$R_{DA} = f(A_{DA}, W_{DA}, Rc_{DA}, Ad_{DA}).$$

При цьому, зазначимо, що живучість S_{DA} електронного архіву *DA* буде визначена як

$$S_{DA} = \lim_{t \to 0} P[F(t) \geq F_{\min} | \exists D(t)],$$

де $F(t)$ — функціональність електронного архіву; $F_{\min}$ — мінімально допустимий рівень функціональності, який повинен забезпечити електронний архів *DA*, щоб вважатися «живим»; $D(t)$ — наявність деструктивного впливу на систему в момент часу *t*; $\lim_{t \to 0}$ — межа у часі, що показує довгострокову здатність до виживання; *P*[.] — імовірність, що функціональність не впаде нижче критичного рівня за умов наявного деструктивного впливу. Типи резильєнтності наведено в табл. 7

Таблиця 7. Типи резильєнтності інформаційно-аналітичних систем обробки даних

Позначення	**Тип резильєнтності**	**Опис**
R_{DA}^{Adapt}	Адаптивна	Перетворення даних у формат, непридатний до прочитання без криптографічного ключа
R_{DA}^{Dyn}	Динамічна	Використання комбінації кількох факторів (пароль, біометрія, токен) для перевірки особи користувача
R_{DA}^{Infra}	Інфраструктурна	Безперервне відстеження та аналіз дій користувачів і систем для виявлення підозрілих аномалій
R_{DA}^{Func}	Функціональна	Регулярне створення копій даних і підтримка їхньої актуальності для відновлення після інцидентів
R_{DA}^{Proc}	Процесуальна	Перевірка відповідності та безпечності вхідних запитів, особливо до AI/LLM модулів
R_{DA}^{Net}	Мережева	Використання моделей поведінки та машинного навчання для виявлення відхилень від нормальних патернів.
R_{DA}^{Org}	Організаційна	Укріплення моделей машинного навчання до атак типу adversarial input або data poisoning.
R_{DA}^{Tech}	Технічна	Накладання прав доступу та ведення журналів активності з подальшим аудитом.
R_{DA}^{Sem}	Семантична	Валідація цифрового підпису документа на основі відкритих сертифікатів або хешів.
R_{DA}^{Oper}	Операційна	Використання криптографічного хешування та перевірки контрольних сум для збереження достовірності метаданих

Відповідність типів резильєнтності $R_{DA}^{[Type]}$ функціям електронних архівів F_{DA} наведено в табл. 8 і Графі 4 (рис. 4).

Таблиця 8. Відповідність типів резильєнтності функціям електронного архіву

	R_{DA}^{Adapt}	R_{DA}^{Dyn}	R_{DA}^{Infra}	R_{DA}^{Func}	R_{DA}^{Proc}	R_{DA}^{Net}	R_{DA}^{Org}	R_{DA}^{Tech}	R_{DA}^{Sem}	R_{DA}^{Oper}
F_{DA_1}	0.5	0.0	1.0	1.0	0.0	1.0	0.5	1.0	1.0	0.0
F_{DA_2}	1.0	1.0	0.0	0.0	0.5	1.0	0.0	0.0	1.0	1.0
F_{DA_3}	1.0	1.0	0.0	0.0	0.0	1.0	1.0	0.0	0.5	1.0
F_{DA_4}	0.5	0.0	0.5	1.0	1.0	1.0	0.5	1.0	0.0	0.5
F_{DA_5}	0.0	0.0	0.5	1.0	0.0	0.5	0.0	1.0	0.5	1.0
F_{DA_6}	0.0	0.0	1.0	1.0	1.0	1.0	0.5	1.0	0.5	0.5
F_{DA_7}	0.0	0.5	0.0	0.5	0.5	0.0	0.0	1.0	1.0	0.5
F_{DA_8}	1.0	0.5	0.5	0.0	0.5	0.0	1.0	0.0	1.0	0.5
F_{DA_9}	1.0	0.5	0.5	1.0	0.5	0.0	0.0	0.5	1.0	0.0
$F_{DA_{10}}$	1.0	0.0	0.0	0.5	0.0	0.5	1.0	0.0	0.5	0.0

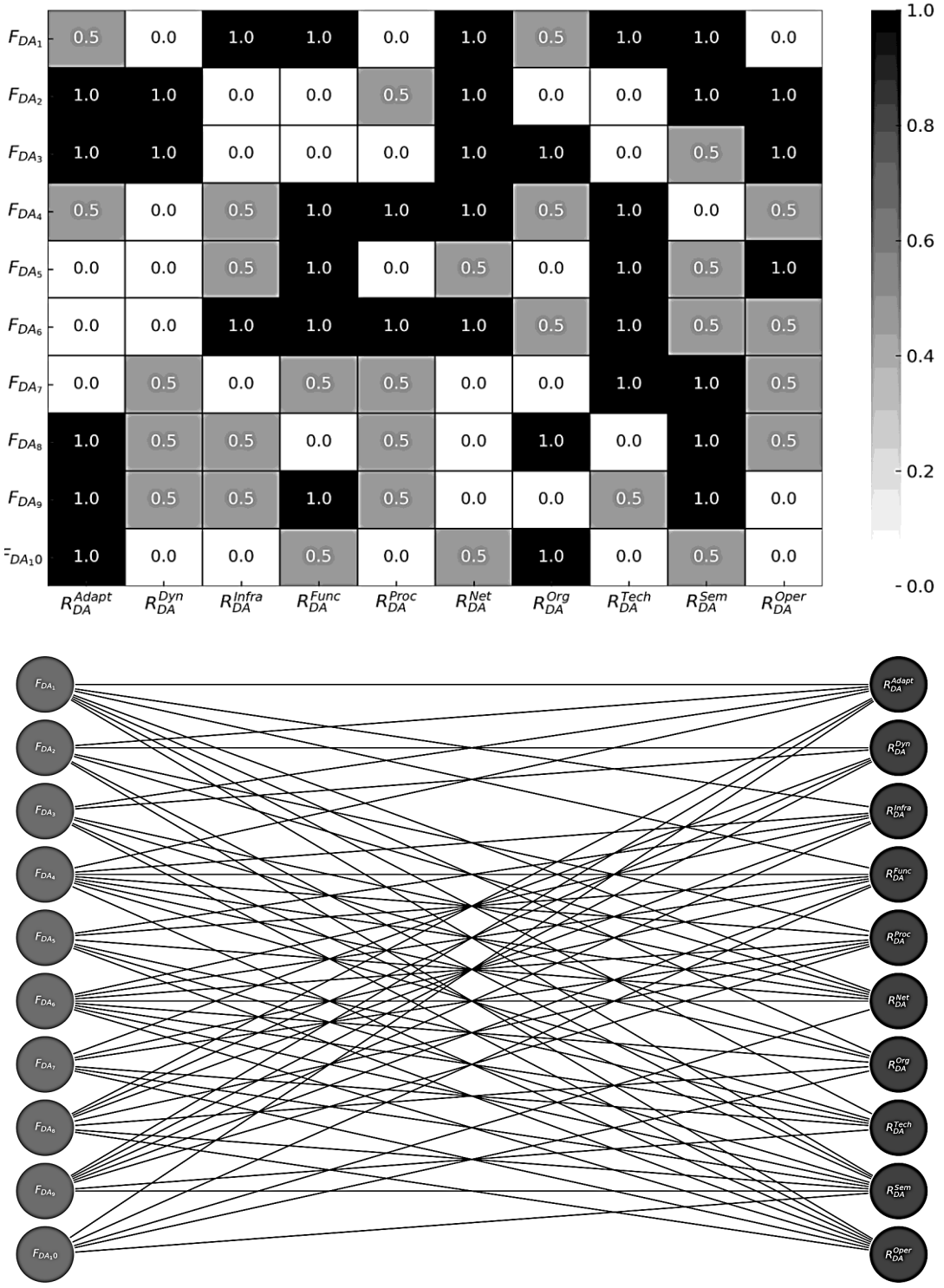

Рис 4. Граф 4 — відповідність типів резильєнтності функціям електронного архіву

Математична формалізація резильєнтності електронних архівів може бути представлена як базова формула резильєнтності в часі *t:*

$$R(t) = \omega_1 \cdot A_{AD}(t) + \omega_2 \cdot W_{AD}(t) + \omega_3 \cdot Rc_{AD}(t) + \omega_4 \cdot Ad_{AD}(t),$$

де $\omega_i \in [0,1]$ та $\sum_{i=1}^{4} \omega_i$=1, а також як альтернативна нормативна формула (через інтеграл ефективності — здатність системи зберігати ефективність функціонування електронного архіву протягом інциденту та після нього):

$$R = \frac{1}{T}\int_0^T \frac{F(t)}{F_{nom}}\partial t,$$

де R — інтегральна резильєнтність за період спостереження T (який включає кіберінцидент, реакцію, відновлення); $F(t)$ — фактична функціональність електронного архіву в часі t; F_{nom} — номінальна (еталонна) функціональність. У такому разі, електронний архів вважається резільєнтним, якщо в часі $t \in [t_0, t_1]$ виконується умова $F(t) \geq \theta \cdot F_{nom}$, $\forall t \in [t_0, t_1]$, де $\theta \in [0,1]$ — мінімальний допустимий рівень функціонування під час або після інциденту — критерій резільєнтного перерізу електронного архіву (Resilience Threshold Function of Digital Archive), а функція відновлення електронного архіву (Resilience Recovery Function of Digital Archive) може бути представлена, як

$$Rc(t) = \frac{F(t) - F_{\min}}{F_{nom} - F_{\min}},$$

де $F_{\min}$ — мінімальна критична функціональність; $Rc(t) \in [0,1]$ — нормована швидкість, або ступінь відновлення електронного архіву.

Резильєнтність електронного архіву визначається не лише логікою його функціонування або політиками безпеки, а й архітектурою інфраструктури, яка забезпечує базові умови для адаптації, відновлення та стійкого функціонування. У цьому контексті доцільно ввести поняття резильєнтної інфраструктури електронного архіву (Resilient Infrastructure of a Digital Archive) як системної властивості ECM/CSP системи, що описує здатність її фізичних, віртуалізованих і логічних компонент підтримувати цілісність, доступність і контрольованість електронних інформаційних ресурсів за наявності деструктивних впливів. Основними елементами такої інфраструктури є: розподілена топологія з резервуванням (георезервування, реплікація даних, кластерні сховища); автоматизовані механізми перемикання (failover) на резервні вузли та канали передачі даних; ізольовані зони безпеки (зони довіри, сегментація мережі, sandboxing для LLM/AI); механізми самодіагностики та самовідновлення (self-healing storage, policy-driven recovery); контроль доступу на основі ролей з динамічними політиками (RBAC/ABAC); інфраструктурна адаптивність — здатність перебудовувати робочі потоки залежно від рівня загроз (наприклад, перехід на офлайн-режим індексації при DoS-атаках). Введення такого поняття дозволяє перейти від аналізу резильєнтності, як суто поведінкової характеристики, до оцінки топологічної та архітектурної готовності архіву до кіберінцидентів, що відкриває можливість стандартизованого аудиту, порівняння та планування розгортання архівних систем у середовищах з підвищеним ризиком.

Живучість S_{DA} електронного архіву *DA* буде визначена як

$$S_{DA} = \lim_{t \to 0} P[F(t) \geq F_{min} | \exists D(t)],$$

де $F(t)$ — функціональність електронного архіву; F_{min} — мінімально допустимий рівень функціональності, який повинен забезпечити електронний архів DA, щоб вважатися «живим»; $D(t)$ — наявність деструктивного впливу на систему в момент часу t; $\lim_{t \to 0}$ — межа у часі, яка показує довгострокову здатність до виживання; $P(\cdot)$ — імовірність, що функціональність не впаде нижче критичного рівня за умов наявного деструктивного впливу.

Математична формалізація живучості електронного архіву на проміжку часу визначається як імовірність того, що при деструктивному впливі функціональність DA не опуститься нижче критичного рівня S_{DA}, який можна представити у вигляді ймовірнісного визначення

$$S_{DA} = P[\forall t \in [t_0, t_1], D(t) = 1 \Rightarrow F(t) \geq \delta],$$

або у вигляді інтегрального визначення

$$S_{DA} = \frac{1}{T} \int_{t_0}^{t_1} \mathbb{I}_{[F(t) \geq \delta]} \cdot D(t) \partial t,$$

де $\mathbb{I}_{[F(t) \geq \delta]}$ — індикаторна функція, значення якої дорівнює 1, або 0, якщо $F(t) \geq \delta$, а $T = t_1 - t_0$.

Позначимо: $F_{DA} = \{F_{DA_1}(t), F_{DA_2}(t), \ldots, F_{DA_n}(t)\}$ — множина функцій електронного архіву в момент часу t; $FT_{DA} = \{FT_{DA_1}(t), FT_{DA_2}(t), \ldots, FT_{DA_m}(t)\}$ — множина активних кіберзагроз у момент часу t; $\Delta_{ij}(t) \in [0,1]$ — ступінь деструктивного впливу загрози FT_{DA_j} на функцію електронного архіву F_{DA_i} в момент часу t; $\rho_i \in [0,1]$ — вагова значущість функції F_{DA_i} для забезпечення (цілісної) резильєнтності; F_i^{nom} — номінальне (еталонне) значення функціональності F_{DA_i}. Тоді, математичну формалізацію впливу кіберзагроз на резильєнтність електронного архіву можна представити у вигляді формули:

$$R_{DA}(t) = \sum_{i=1}^{n} \rho_i \cdot \frac{F_{DA_i}(t) \cdot \left(1 - \sum_{j=1}^{m} \Delta_{ij}(t) \cdot \mathbb{I}_{\left[FT_{DA_j}(t)=1\right]}\right)}{F_{DA_i}^{nom}}.$$

Слід зазначити, що кожна функція F_{DA_i} модулюється впливом загроз, актуальних у даний момент часу. Сукупний деструктивний ефект на функцію F_{DA_i} можна представити виразом:

$$\sum_{j=1}^{m} \Delta_{ij}(t) \cdot \mathbb{I}_{[T_j(t)=1]}.$$

Нормалізація F_i^{nom} дозволяє оцінювати втрату ефективності відносно номінального стану; зважена по i сума дозволяє враховувати різну важливість функцій для загального рівня резильєнтності.

У цій статті автори формалізують загальний випадок, а перелік конкретних функцій F_{DA_i}, а також деталізованих моделей впливу загроз FT_{DA_j} і матриці впливів Δ_{ij} може бути предметом окремого дослідження.

Резильєнтність інформаційних систем, у загальному випадку, може розглядатись як інтегральна характеристика, що відображає її реакцію на одиничний інцидент або сталий вплив. Однак електронний архів, як динамічна інформаційна система, функціонує у середовищі змінного ландшафту загроз, що вимагає адаптивної резильєнтності електронного архіву (Adaptive Resilience of a Digital Archive) — здатності ECM/CSP-системи змінювати власні параметри, конфігурації і політики реагування залежно від характеру загроз, історії інцидентів й ефективності попередніх протидій. Формально, адаптивну резильєнтність архіву $R_{DA}(t)$ можна представити як функцію, що еволюціонує у часі залежно від: поточного рівня функціональності $F_{DA}(t)$; градієнта змін деструктивного впливу $\nabla D(t)$; адаптаційної поведінки системи $\mathcal{A}_{DA}(t)$, що включає перемикання режимів, активацію резервних механізмів, зміну конфігурацій захисту тощо. Математично це можна записати у вигляді динамічного рівняння

$$R_{DA}(t + \Delta t) = f(F_{DA}(t), \nabla D(t), \mathcal{A}_{DA}(t)),$$

де $f(\cdot)$ — функція адаптації, що моделює поведінкову реакцію системи на загрозу. Таким чином, адаптивна резильєнтність — це не фіксована метрика, а еволюційний процес підтримки стійкого функціонування в умовах змінної агресії, що робить її придатною для застосування в умовах постійного впливу кіберзагроз. Динамічну резильєнтність електронного архіву (Dynamic Resilience of a Digital Archive) можна представити, як функцію зворотного зв'язку:

$$F_{DA}(t + \Delta t) = f(F_{DA}(t), \nabla D(t), \mathcal{A}_{DA}(t)),$$

де $\mathcal{A}_{DA}(t)$ — функція адаптації.

Після кіберінциденту або стресового впливу ефективне відновлення функціональності електронного архіву є визначальним чинником його довготривалої резильєнтності. Для кількісного опису цього процесу вводиться поняття профілю відновлення електронного архіву (Recovery Profile of a Digital Archive) — функції, що відображає зміну ступеня відновлення критичних компонентів системи у часі після інциденту. Нехай електронний архів складається з n критичних компонентів (функцій, сервісів або підсистем), кожна з яких має власну динаміку відновлення. Позначимо: $r_i(t) \in [0,1]$ — ступінь відновлення i-ї компоненти на момент часу t після інциденту (0 — не відновлено, 1 — повне відновлення); $\omega_i \in [0,1]$ — ваговий коефіцієнт значущості цієї компоненти у загальному функціонуванні системи $\omega_i \in [0,1]$; t_0 — момент завершення кіберінциденту (початок поновлення). Тоді профіль відновлення електронного архіву визначається як

$$R_{rec}(t) = \sum_{i=1}^{n} \omega_i \cdot r_i(t),$$

де $t \geq t_0$. Ця функція описує сукупний рівень відновлення електронного архіву d часі, забезпечуючи оцінку швидкості реакції — похідна $\frac{d}{dt} R_{rec}(t)$, яка інтерпретується як темп відновлення; виявлення вузьких місць — компоненти з уповільненим

зростанням $r_i(t)$ і високими вагами ω_i визначають критичні зони ризику; планування автоматизованих сценаріїв — профіль, який може бути використаний для побудови політик пріоритетного відновлення (наприклад, на основі SLA). Профіль відновлення є необхідним аналітичним інструментом для динамічного управління відновленням електронного архіву (Business Continuity Planning of Digital Archive, BCP) відповідно до політик безперервності архівної діяльності та підвищення загальної резильєнтності.

Модель

Для реалізації мережевої моделі резильєнтності електронного архіву авторами запропоновано код програми мовою програмування R (Додаток 1), яка:

— будує мережеву модель електронного архіву з матриць «Процеси – Загрози – Протидії»;

— відображає граф взаємозв'язків (вузли: процеси/загрози/протидії; ребра: наявність впливу/контрдії);

— моделює атаку (вимкнення обраних вузлів), ітеративне відновлення та профіль відновлення $F_{DA}(t)$;

— обчислює час повного відновлення t_r (критерій резильєнтності) та інтегральну резильєнтність R.

На основі матриць «Процеси – Загрози – Протидії» будується граф взаємозв'язків, моделюється вплив кібератаки та відновлення компонент архіву. Розраховуються профіль відновлення $F_{DA}(t)$, час повного відновлення t_r (критерій резильєнтності) та інтегральна резильєнтність:

$$R = \frac{1}{T+1}\sum_{T}^{t=0}\frac{F_{DA}(t)}{F_{DA}^{0}},$$

Параметри моделі θ, швидкості відновлення, сценарії атак можуть бути змінені для аналізу різних конфігурацій архіву.

Висновки

Наукова новизна роботи полягає у формалізації резильєнтності електронних архівів через введення критерія резільєнтного перерізу, функції відновлення та профілю відновлення. У роботі здійснено системний аналіз і запропоновано математичну формалізацію поняття резильєнтності електронних архівів. Розглянуто критерій резільєнтного перерізу та функцію відновлення електронного архіву. Введено поняття резільєнтної інфраструктури електронного архіву. Запропоновано математичну формалізацію адаптивної і динамічної резильєнтності електронних архівів. Введено поняття профілю відновлення та описано функцію сукупного рівня відновлення електронного архіву. Ці аспекти надають можливість кількісно оцінювати резильєнтність електронних архівів, здатність архіву витримувати вплив деструктивних подій і відновлювати свою функціональність. Запропоновані моделі можуть бути покладені в основу методик оцінювання резильєнтності та впровадження політик безперервності діяльності в системах класу ECM/CSP і практично використані для побудови методик оцінювання та підвищення резильєнтності електронних

архівів. Подальші дослідження доцільно зосередити на адаптації моделей до конкретних архівних платформ, аналізі сценаріїв впливу кіберзагроз і реалізації засобів автоматизованого управління відновленням архівів на основі профілю відновлення. Таким чином, результати роботи створюють основу для подальших досліджень і практичного впровадження політик безперервності діяльності в електронних архівах.

1. ISO 22316:2017. Security and resilience — Organizational resilience — Principles and attributes. — Geneva: International Organization for Standardization, 2017. 16 p. URL: https://www.iso.org/standard/50053.html

2. Ross R., Pillitteri V., Graubart R., McEvilley M., Saydjari O. Developing Cyber Resilient Systems: A Systems Security Engineering Approach (Second Public Draft). — Gaithersburg, MD: National Institute of Standards and Technology, 2021. 262 p. (NIST Special Publication; 800–160, Vol. 2, Rev. 1). DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1.

3. Додонов А. Г., Ландэ Д. В. Живучесть информационных систем. Киев: Наук. думка, 2011. 256 с. (Серія: Проблеми інформаційної безпеки). ISBN 978-966-00-1145-7. URL: http://dwl.kiev.ua/art/zhm/zhyvuchest.pdf

4. Gartner. Definition of Content Services Platform (CSP). 2017. Retrieved from https://www.gartner.com/en/information-technology/glossary/content-services-platform-csp

5. Knight J.C., Strunk E.A., Sullivan K.J. Towards a rigorous definition of information system survivability. Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX 2003). IEEE, 2003. Vol. 1. P. 78–89. DOI: 10.1109/DISCEX.2003.1194875. URL: https://ieeexplore.ieee.org/document/1194875

6. Mead Nancy R., et al. Survivability: Protecting Your Critical Systems. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1999. 24 p. (CMU/SEI Report ; CMU/SEI-99-TN-017). URL: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=513779

7. Tsyrulnev Yu. Cybersecurity of Intellectual Information Aggregation Processes into Digital Archives. Theoretical and Applied Cybersecurity. 2025;2. (Intelligent Data Analysis Methods in Cybersecurity). DOI: https://doi.org/10.20535/tacs.2664-29132025.2.343769.

Додаток 1

Вихідний код програми мовою R для реалізації моделювання резильєнтності електронного архіву:

```
suppressWarnings({
  if (!require(igraph)) install.packages("igraph", repos="https://cloud.r-project.org")
  if (!require(readr))  install.packages("readr",  repos="https://cloud.r-project.org")
})
library(igraph); library(readr)

# 1) Завантаження матриць (приклади назв файлів; підставте свої)
# process_threat.csv: rows=Processes, cols=Threats, values {0,1}
# threat_counter.csv: rows=Threats,  cols=Counters, values {0,1}
# process_counter.csv: rows=Processes, cols=Counters, values {0,1} (необов'язкова)
M_PT <- as.matrix(read_csv("process_threat.csv", show_col_types = FALSE)[,-1])
M_TC <- as.matrix(read_csv("threat_counter.csv", show_col_types = FALSE)[,-1])

proc_names   <- read_csv("process_threat.csv", show_col_types = FALSE)[[1]]
threat_names <- colnames(read_csv("process_threat.csv", show_col_types = FALSE)[,-1])
counter_names<- colnames(read_csv("threat_counter.csv", show_col_types = FALSE)[,-1])
```

```
# 2) Побудова багатошарового графа (P, T, C)
# Вершини
V_proc   <- paste0("P:", proc_names)
V_thr    <- paste0("T:", threat_names)
V_count  <- paste0("C:", counter_names)
V_all    <- c(V_proc, V_thr, V_count)
g <- make_empty_graph() + vertices(V_all, type=c(rep("P",length(V_proc)),
                                                 rep("T",length(V_thr)),
                                                 rep("C",length(V_count))))
# Ребра P–T
E_PT <- which(M_PT==1, arr.ind = TRUE)
if (nrow(E_PT)>0) {
  edges_PT <- as.vector(rbind(V_proc[E_PT[,1]], V_thr[E_PT[,2]]))
  g <- g + edges(edges_PT)
}
# Ребра T–C
E_TC <- which(M_TC==1, arr.ind = TRUE)
if (nrow(E_TC)>0) {
  edges_TC <- as.vector(rbind(V_thr[E_TC[,1]], V_count[E_TC[,2]]))
  g <- g + edges(edges_TC)
}

# 3) Візуалізація мережі (кольори за типом)
type <- V(g)$type
cols <- ifelse(type=="P","steelblue", ifelse(type=="T","tomato","darkseagreen"))
set.seed(1)
layout <- layout_with_fr(g)
plot(g, layout=layout, vertex.color=cols, vertex.size=18, vertex.label.cex=.75,
     main="Мережева модель резильєнтності електронного архіву")

# 4) Динаміка відновлення
# Стан вузлів: процеси P впливають на F_DA(t) (інші — допоміжні).
P_idx <- which(type=="P"); T_idx <- which(type=="T"); C_idx <- which(type=="C")
Np <- length(P_idx)
stateP  <- rep(1.0, Np)  # F_i(t) для процесів
targetP <- rep(1.0, Np)
rateP   <- rep(0.25, Np) # базова швидкість відновлення

F_DA <- function(st) mean(st)
F0   <- F_DA(stateP)

# 5) Сценарій атаки: знеструмлюємо процеси, що пов’язані з найбільш агресивними загрозами
# Приклад: знаходимо загрозу з найбільшою ступінню і "гасимо" суміжні процеси
degT <- degree(induced_subgraph(g, V(g)[T_idx]))
worstT <- T_idx[ which.max(degT) ]
affectedP <- intersect(P_idx, neighbors(g, worstT))
if (length(affectedP)==0) affectedP <- sample(P_idx, 1)
stateP[ match(affectedP, P_idx) ] <- 0.0

# 6) Порогова залежність через сусідство з контрдіями (T–C) та іншими P
theta <- 0.7   # поріг резільєнтного перерізу
Tmax  <- 20
F_series <- numeric(Tmax+1)
R_int <- 0.0
t_r <- NA
```

```
stepRecover <- function(stateP) {
  next <- stateP
  for (k in seq_along(P_idx)) {
    u <- P_idx[k]
    # оцінка "підтримки" вузла: середній стан суміжних процесів + наявність контрдій через загрози
    nbrP <- intersect(P_idx, neighbors(g, u))
    depP <- if (length(nbrP)==0) 1.0 else mean(stateP[ match(nbrP, P_idx) ])

    # якщо для процесу існують загрози, для яких є контрдії, — прискорюємо відновлення
    nbrT <- intersect(T_idx, neighbors(g, u))
    hasCounter <- FALSE
    if (length(nbrT)>0) {
      for (t in nbrT) {
        if (length(intersect(C_idx, neighbors(g, t)))>0) { hasCounter <- TRUE; break }
      }
    }
    coef <- ifelse(depP >= theta, 1.0, 0.5) * ifelse(hasCounter, 1.2, 1.0)
    r <- min(1, rateP[k] * coef)
    next[k] <- min(targetP[k], stateP[k] + r*(targetP[k]-stateP[k]))
  }
  next
}

for (t in 0:Tmax) {
  Ft <- F_DA(stateP); F_series[t+1] <- Ft; R_int <- R_int + Ft/F0
  if (is.na(t_r) && Ft >= F0 - 1e-9) t_r <- t
  if (t < Tmax) stateP <- stepRecover(stateP)
}
R_int <- R_int / (Tmax+1)

# 7) Профіль відновлення
par(mfrow=c(1,1), mar=c(4,4,2,1))
plot(0:Tmax, F_series/F0, type="l", lwd=2,
     xlab="t", ylab=expression(F[DA](t)/F[DA]^0),
     main="Профіль відновлення F_DA(t)")
abline(h=1, lty=2)
legend("bottomright", legend=sprintf("t[r]=%s,  R=%.3f",
       ifelse(is.na(t_r),"—",t_r), R_int), bty="n")
```

Надійшла до редакції 01.09.2025