КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1260
УДК 004.056.5

Дрейс Юрій Олександрович
кандидат технічних наук, доцент
доцент кафедри системного аналізу та інформаційних технологій
Маріупольський державний університет, Київ, Україна
ORCID: 0000-0003-2699-1597
y.dreis@mu.edu.ua

СТРУКТУРНА МОДЕЛЬ СИСТЕМИ ОЦІННЮВАННЯ НАСЛІДКІВ ВИТОКУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

Анотація. У статті представлено структурну модель системи оцінювання наслідків витоку інформації з обмеженим доступом, яка спрямована на підвищення рівня інформаційної безпеки людини, суспільства, держави. Система дозволяє автоматизувати процес: ідентифікації та класифікації публічної (відкритої) інформації та тієї, доступ до якої обмежено (інформацію з обмеженим доступом); аналізу ризиків з прогнозуванням потенційних наслідків (шкоди, збитків) від можливого або вже здійсненого витоку персональних даних, службової інформації, державної таємниці (та/або втрати їх матеріальних носіїв) і мінімізувати фінансові втрати та/або інші тяжкі наслідки; формування реєстру порушень і класифікатора об’єкта критичної інформаційної інфраструктури. Відповідно до наявних вимог щодо особливостей організації режиму секретності та доступу до окремих видів класифікованої інформації, розроблена структура системи включає підсистему оцінювання наслідків витоку персональних даних (за національним і міжнародним законодавством у т.ч. GDPR) і підсистему оцінювання наслідків витоку службової інформації та/або державної таємниці. Запропонована система забезпечує оцінювання ефективності функціонування систем захисту інформації (комплексної системи захисту інформації та/або системи охорони державної таємниці) об’єкта критичної інфраструктури, суб’єкта владних повноважень та режимно-секретної діяльності та призначена для використання державним експертом з питань таємниць, судово-експертними установами, комісією по роботі зі службовою інформацією, іншими уповноваженими особами.

Ключові слова: захист інформації; інформація з обмеженим доступом; оцінювання наслідків (шкоди, збитків); персональні дані; службова інформація; державна таємниця; ризики; об’єкт критичної інфраструктури; модель; система підтримки прийняття рішення; витік інформації.

ВСТУП

Актуальність розробки системи оцінювання наслідків (шкоди, збитків) витоку інформації з обмеженим доступом (ІзОД) обумовлена зростаючою кількістю загроз та атак на об’єкти критичної інфраструктури (ОКІ) держави. ІзОД є цінним інформаційним активом та стратегічним ресурсом для функціонування об'єктів критичної інформаційної інфраструктури (ОКІІ), які забезпечують надання ОКІ основних послуг та/або виконання життєво важливих функцій (ОП/ЖВФ) у секторах і галузях критичної інфраструктури. А постійне зростання обсягів ІзОД та її використання ОКІІ супроводжується активним посиленням кіберзагроз, помилками персоналу, втратою носіїв інформації або появою нових вразливостей у системі, які можуть призвести до її витоку, несанкціонованого доступу, маніпуляцій, компрометації або знищення. Витоки ІзОД спричиняють значні негативні наслідки, фінансові втрати та економічні збитки як ОКІ, так і державі у цілому, у т.ч. й інші тяжкі наслідки, включаючи штрафи за порушення нормативних вимог, можливі судові витрати та компенсації постраждалим. Тому, головною законодавчою вимогою до ОКІІ наразі є ефективне забезпечення стійкого і безперервного функціонування ОКІ для надання ним ОП/ЖВФ, реалізовуючи при цьому захист ОКІІ від загроз, кібератак, кіберінцидентів та інцидентів захисту ІзОД. Ефективність захисту ОКІІ визначається її здатністю до своєчасного виявлення, запобігання і нейтралізації загроз безпеці ОКІ, а також мінімізацію та ліквідацію наслідків у разі їх реалізації шляхом впровадження системи захисту інформації в системі.

Деякі ОКІ, наприклад особливо важливі об’єкти держави (підприємства, установи та організації), незалежно від їх форми власності мають стратегічне значення для економіки та безпеки, забезпечують життєдіяльність населення або функціонування органів влади, а тому підлягають постійній охороні та захисту. А порушення роботи цих об'єктів може призвести до надзвичайних ситуацій, значних економічних збитків або загрози обороноздатності країни. А тому є виведення з ладу таких ОКІ або припинення функціонування їх ОКІІ для втрати контролю та управління державою над цими ОКІ шляхом завдання їй серйозних економічних збитків, соціального напруження і паніки, спричинених неможливістю ними подальшого надання ОП/ЖВФ і є основною метою сучасних кіберзагроз та кібератак.

У період перебування України у військовому стані досить гостро постає питання у забезпеченні безпеки усіх її ОКІ від можливої загрози витоку ІзОД внаслідок реалізації кібератак та кіберінцидентів, несанкціонованого втручання та кризових ситуацій, тобто у необхідності підтримки такого стану захищеності ІзОД в системі, за якого ОКІІ забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість ОКІ до надання ОП/ЖВФ, порушення яких призведе до негативних наслідків (шкоди, збитків) для національної безпеки і оборони, наприклад, постачання електроенергії, води, тепла, газу тощо. Саме тому, у більшості законодавчих та регуляторних актах, де встановлюються умови для віднесення ОКІ та/або їх ОКІІ, де обробляється та циркулює ІзОД до певної категорії критичності з виконанням вимог до її захисту, закладені критерії орієнтовані на визначення і оцінювання можливих потенційних наслідків (шкоди) у разі її витоку.

У зв’язку із вищезазначеним актуальною задачею є розробка моделі системи оцінювання наслідків витоку ІзОД ОКІ, що спрямована на автоматизацію ключових процесів аналізу ризиків, прогнозування можливої шкоди і оцінювання завданих збитків, розробку експертних висновків і надання рекомендацій щодо заходів для їх мінімізації. Використання такої системи буде сприяти покращенню рівня захисту ІзОД, зниженню фінансових ризиків і потенційних наслідків (шкоди, збитків), забезпеченню відповідності ОКІ та ОКІІ сучасним нормативним вимогам у сферах інформаційної безпеки, захисту інформації та кібербезпеки.

Постановка проблеми. Відповідно до вимог вітчизняного і міжнародного законодавства у сфері захисту класифікованої інформації (персональних даних (ПД)), службової інформації (СлІ), державної таємниці (ДТ)), управління ризиків та оцінка збитків, пов’язаних з порушенням втрати їх конфіденційності, є важливими і актуальними питаннями для кожної людини, організації, держави. У цьому контексті постає необхідність створення системи, яка б оцінювала можливі негативні наслідки (шкоду, збитки) витоку ПД, СлІ або ДТ ОКІ за цими вимогами.

Призначення та основні задачі системи:

– автоматизована ідентифікація і класифікація публічної інформації на відкриту та ІзОД, а саме на ПД, СлІ, ДТ за наборами параметрів розроблених раніше моделей;

– інтеграція і адаптація існуючих сучасних моделей систем оцінювання негативних наслідків втрати ІзОД;

– розрахунок потенційних фінансових втрат, істотної шкоди (збитків) та/або інших тяжких наслідків через порушення конфіденційності окремо для ПД, СлІ і ДТ, у т.ч. через терористичні акти, з урахуванням процесу старіння інформації;

– оцінка рівня зниження ефективності комплексної системи захисту інформації (КСЗІ) або системи охорони ДТ (СОДТ) від розголошення, втрати чи витоку ІзОД;

– підготовка обґрунтування щодо застосування адміністративної (ПД, СлІ) чи/або кримінальної відповідальності з відшкодуванням збитків національній безпеці (ДТ) за результатами оцінки наслідків їх витоку, внаслідок вчинення правопорушення;

– розробка програмного забезпечення для автоматизованого збору та аналізу даних про наслідки витоку ПД і окремо для СлІ та/або ДТ.

– формування рекомендацій до політики інформаційної безпеки ОКІ та до плану кібербезпеки їх ОКІІ для мінімізації ризиків витоку ІзОД і запобігання майбутнім порушенням конфіденційності.

Мета постановки проблеми – створити інтегровану систему, яка дозволяє ОКІ, суб’єктам владних повноважень (СВП) та/або суб’єктам режимно-секретної діяльності (СРСД) (далі по тексту їх буде узагальнено як ОКІ), відповідати високим стандартам захисту ІзОД, знизити ризики порушення її конфіденційності та мінімізувати негативні наслідки для людини, суспільства та національної безпеки держави.

Аналіз останніх досліджень і публікацій. У даному дослідженні проведено аналіз наукових праць вітчизняних вчених у яких започатковано розв’язання проблеми з одного боку, – щодо методологічних, організаційних та юридичних засад забезпечення стійкого функціонування ОКІ, захисту ІзОД та підстав для її класифікації (Д. Бобро, В. Горбулін, О. Єрменчук, І. Касперський, С. Кондратов, О. Суходоля,

С. Фальченко та ін.) [1-5], а з іншого, – щодо побудови систем, методів, засобів і заходів захищеної обробки інформації, оцінювання ризиків та наслідків (шкоди) втрати інформаційних ресурсів (О. Архипов, С. Гончар, О. Корченко, С. Казмірчук, О. Потій, В. Слюсар та ін.) [5-28], а також міжнародного та вітчизняного інформаційного законодавства [29-32].

Метою роботи є розробка та обґрунтування структурної моделі системи оцінювання наслідків (шкоди, збитків) витоку ІзОД, що дозволить виявляти, аналізувати та прогнозувати потенційні ризики, пов'язані з втратою їх конфіденційності, з метою своєчасної мінімізації та ліквідації цих наслідків, необхідної для забезпечення стійкого та безперервного функціонування ОКІ для надання ним ОП/ЖВФ відповідно до вимог сучасного законодавства і стандартів інформаційної безпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Структурна модель системи оцінювання наслідків витоку ІзОД. На основі розробленої моделі ідентифікації [16, 25, 28] і методів нечіткої класифікації ІзОД [4, 15, 26], моделі та методу оцінки ризиків захисту ПД під час їх обробки в автоматизованих системах [8, 27], теоретико-множинної GDPR-моделі параметрів ПД [12], моделі параметрів оцінювання наслідків витоку СлІ ОКІ [17], моделі оцінювання наслідків витоку ДТ від кібератак на критичну інформаційну інфраструктуру держави [11], моделей формування бази даних параметрів для оцінювання стану охорони ДТ [13, 19-22], моделі класифікатора [10] і методу оцінювання наслідків втрати ОКІІ [9, 18], удосконаленого методу оцінювання шкоди у разі витоку ДТ [23], методу оцінювання шкоди у разі витоку СлІ [24], а також структурної моделі системи оцінки негативних наслідків втрати ПД [14], розроблено структурну модель системи оцінювання наслідків витоку ІзОД (рис. 1), яка містить:

– блок ідентифікацій і класифікації інформації (БІКІ);
– блок обробки національних параметрів ПД (БОНППД);
– блок формування та зберігання даних (удосконалений) для ПД (БФЗДу(ПД));
– блок визначення рівня порушення та оцінки ризиків (БВРПОР);
– блок формування експертної інформації (БФЕІ);
– блок обробки експертних даних (удосконалений) (БОЕДу);
– блок обробки параметрів СлІ (БОПСлІ);
– блок обробки параметрів СОДТ (БОПСОДТ);
– блок оцінювання параметрів шкоди (БОПШ);
– блок зберігання даних та формування висновку і реєстру порушень (для СлІ/ДТ) (БЗДФВРП(СлІ/ДТ));
– блок формування класифікатора ОКІІ (БФКОКІІ).

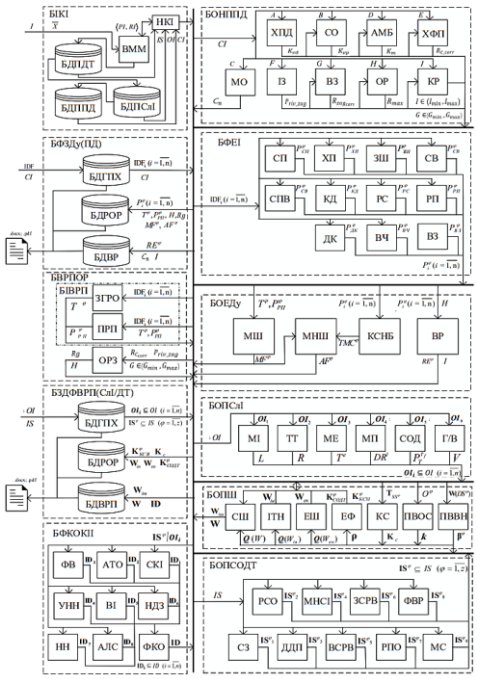

Рис. 1. Структурна модель системи оцінювання наслідків витоку ІзОД

Система оцінювання наслідків витоку ІзОД ОКІ, враховуючи вимоги законодавства щодо обмеження доступу інформації і режиму секретності, складається з: підсистеми оцінювання наслідків витоку ПД (за національним і міжнародним законодавством) та підсистеми оцінювання наслідків витоку СлІ та/або ДТ.

Підсистема оцінювання наслідків витоку ПД складається з контуру оцінювання наслідків витоку ПД відповідно до вимог національного законодавства (БІКІ, БОНППД, БФКОКІІ), а також з контуру оцінювання наслідків витоку ПД відповідно до вимог міжнародного законодавства до складу якого інтегровано та удосконалено існуючу структурну модель системи оцінки негативних наслідків витоку ПД [14] за Регламентом GDPR (БВРПОР, БОЕДу, БФЗДу(ПД), БФЕІ). Тому у цілому підсистема містить такі блоки як: БІКІ, БОНППД, БВРПОР, БОЕДу, БФЗДу(ПД), БФЕІ, БФКОКІІ.

Підсистема оцінювання наслідків витоку СлІ та/або ДТ складається з контуру оцінювання наслідків витоку СлІ (БІКІ, БОПСлІ, БОПШ, БФКОКІІ, БЗДФВ(СлІ/ДТ)) та контуру оцінювання наслідків витоку ДТ (БІКІ, БОПСОДТ, БОПШ, БФКОКІІ, БЗДФВ(СлІ/ДТ)) відповідно до вимог національного законодавства, а тому у цілому містить такі блоки як: БІКІ, БОПСлІ, БОПСОДТ, БОПШ, БФКОКІІ, БЗДФВ(СлІ/ДТ).

БІКІ служить для нечіткої ідентифікації та класифікації публічної інформації на відкриту та ІзОД і складається з:

– бази даних параметрів ДТ (БДПДТ) – містить параметри для ідентифікації відомостей, що становлять ДТ (IS);

– бази даних параметрів СлІ (БДПСлІ) – містить параметри для ідентифікації відомостей, що містять СлІ (OI);

– бази даних параметрів ПД (БДППД) – містить параметри для ідентифікації відомостей, що містять ПД (CI);

– модуль великих мовних моделей (ВВМ) – алгоритми штучного інтелекту синтаксичного пошуку, глибокого аналізу змісту та контексту тексту (за ключовими словами, шаблонами тощо) для виявлення ПД (CI), СлІ (OI) та/або ДТ (IS) (наприклад, як Local LLMs для уникнення передачі чутливих даних стороннім сервісам, мінімізуючи ризики їх витоку [26]).

– модуля нечіткої класифікації інформації (НКІ) – виокремлення з вхідної інформації (I**)** таких відомостей ($\overline{X}$), які за базами даних параметрами ідентифікації ІзОД відносяться до відкритої інформації (PI) чи до одного з видів ІзОД **(**RI**)**, у т.ч. за допомогою модуля ВВМ.

БОНППД – складається з модулів оцінювання та вибору національних параметрів і характеристик витоку ПД (склад та зміст ПД (ХПД), середовище обробки бази ПД в системі (СО), аудит застосованих механізмів безпеки (АМБ), існуючі функціональні послуги безпеки (ХПБ), мета обробки ПД (МО), ідентифікація загроз обробки ПД в системі (ІЗ), величина можливих збитків від втрати ПД (ВЗ), оцінка ризику захисту ПД в системі (ОР), керування ризиком та досягнення необхідного рівня гарантій захисту ПД (КР)), що засновується на конкретних оцінках діяльності ОКІ <A, B, C, D, E, F, G, H, I>, які в результаті сформують значення показників K_{vd}, K_{vp}, K_m, C_n, R_{C_corr}, P_{riv_zag}, R_{max}, $R_{zag_{corr}}$, $I \in (I_{min}, I_{max})$ та $G \in (G_{min}, G_{max})$, що в подальшому буде використано для обчислення сукупних наслідків (шкоди, збитків) φ-го ОКІ.

БВРПОР складається з:

– модулів ЗГРО і ПРП блоку БІВРП структурної моделі системи оцінки негативних наслідків витоку ПД за GDPR, призначення яких описано в [14];

– модуля визначення оцінки ризику захисту ПД в автоматизованій системі (далі – АС) (ОРЗ) – розраховує показник ризику (H) як ймовірність реалізації загрози (P) до виду і величини завданих збитків (G) від можливої втрати ПД, у т.ч. за вартісною (грошовою) (Rg) шкалою.

БФЗДу(ПД) служить для підготовки даних для формування експертного висновку, заснованих на результатах роботи модулів і судженнях експертів, який удосконалено до вимог національного законодавства з питань захисту ПД та складається з:

– бази даних групи питань і характеристик (БДГПХ) – містить питання (IDF^{φ}) та характеристик ПД (CI) для аналізу ризиків і загроз;

– бази даних результатів опитувань і розрахунків (БДРОР) – включає зібрані відповіді експертів P_i^{φ} і результати розрахунків параметрів оцінювання збитків $G \in (G_{min}, G_{max})$ та їх характеристик T^{φ}, MF^{φ}, AF^{φ}, P_i^{φ}, Rg;

– бази даних висновків і рекомендацій (БДВР) – зберігає висновки щодо оцінювання наслідків (Rg) та пропозиції (I, RE^{φ}) щодо мінімізації ризиків.

БЗДФВРП(СлІ/ДТ) служить для підготовки даних для формування експертного висновку та реєстру порушень режиму секретності, заснованих на результатах роботи модулів і судженнях експертів за вимогами національного законодавства у сферах захисту СлІ та ОДТ, який складається з:

– бази даних параметрів і характеристик (БДГПХ) – містить питання та характеристики СлІ (OI) та/або ДТ (IS) для оцінки ефективності стану СОДТ або КСЗІ;

– бази даних результатів опитувань і розрахунків (БДРОР) – включає зібрані відповіді експертів OI_i^{φ} та/або IS_i^{φ} і результати розрахунків параметрів оцінювання шкоди (збитків) (W / $W_{iш}$) та інших параметрів характеристик ($W_{ін}$, $W_{ек}$, $K_{КСЗІ}^{\varphi}$ / $K_{СОДТ}^{\varphi}$);

– бази даних висновків і реєстр порушень з класифікатором ОКІІ (БДВРП) – зберігає висновки щодо оцінювання наслідків (W / $W_{iш}$) з класифікатором ОКІІ (ID^{φ}) у реєстрі порушень режиму секретності φ-ого ОКІ.

БОПСлІ – складається з модулів оцінювання та вибору параметрів і характеристик СлІ (множина ідентифікаторів наявності СлІ на ОКІ (МІ); параметри «трискладового тесту» для встановлення СлІ (ТТ); нечітких (лінгвістичних) еталонів, що відображають судження експерта відносно наявності базових параметрів можливої шкоди (по типу процедури віднесення відомостей до IS) із підмножини R для обмеження доступу (МЕ); множина базових детекційних правил, причинно-наслідкових і просторово-часових характеристик та ознак для СлІ (МП), наприклад, об'єкт цих відомостей, його характеристики, або/та його окремі показники чи їх сукупність тощо; строк обмеження доступу (СОД); ідентифікатори грифу та/або відмітки, що використовуються для обмеження доступу до СлІ (Г/В), що засновується на конкретних оцінках діяльності ОКІ/СВП/СРСД, які в результаті сформують значення показників L , R , T_i^e , DR^l , $P_{\tau_f}^l$, V і у подальшому їх буде використано для обчислення сукупних наслідків (шкоди, збитків) φ-го ОКІ.

БОПСОДТ – складається з модулів оцінювання та визначення параметрів: первинних (суб'єкта звітування, його підпорядкування та відомчу належність (СЗ) режимно-секретного органу, фінансування заходів з ОДТ (РСО)); внутрішніх (наявності у працівників суб'єкта звітування допуску та доступу до ДТ (ДДП), кількості матеріальних носіїв секретної інформації (МНСІ)); вторинних (виконання (наукового та/або науково-технічного супроводження) секретних науково-дослідних, дослідно-конструкторських, проектних та інших наукових робіт, виготовлення секретних виробів (ВСРВ), замовлення (наукового та/або науково-технічного супроводження) секретних науково-дослідних, дослідно-конструкторських, проектних та інших наукових робіт, виготовлення секретних виробів (ЗСРВ), режимні приміщення, об'єкти інформаційної діяльності (РПО), факти втрат МНСІ або розголошення відомостей, що становлять державну таємницю, а також інформації з обмеженим доступом іноземних держав або міжнародних організацій (ФВР), міжнародного співробітництва (МС)), що засновується на конкретних оцінках діяльності ОКІ, які в результаті сформують значення показників N^{φ} , A^{φ} , CD^{φ} , O^{φ} , SU^{φ} , CO^{φ} , CU^{φ} , DS^{φ} , P^{φ} , AP^{φ} , SD^{φ} , E^{φ} , RS^{φ} , NA^{φ} , FP^{φ} , nE^{φ} , nP^{φ} , FA^{φ} , nPN^{φ} , nA^{φ} , nSA^{φ} , nRA^{φ} , nWR^{φ} , nGA^{φ} , nWA^{φ} , SS^{φ} , aM^{φ} , nsM^{φ} , nrM^{φ} , nMr^{φ} , nMt^{φ} , nMf^{φ} , sU^{φ} , nMu^{φ} , tW^{φ} , SW^{φ} , nSW^{φ} , pSW^{φ} , tP^{φ} , SP^{φ} , nSP^{φ} , pSP^{φ} , nRR^{φ} , nCO^{φ} , nCS^{φ} , nD^{φ} , nL^{φ} , nDL^{φ} , nRD^{φ} , nDR^{φ} , nFA^{φ} , nFT^{φ} і у подальшому їх буде використано для обчислення сукупних наслідків (шкоди, збитків) φ-го ОКІ.

БОПШ – складається з модулів оцінювання та визначення (скупної та/або потенційної істотної шкоди (СШ); шкоди від настання інших тяжких наслідків (ІТН), завданої економічної шкоди (збитків) (ЕШ); ефективності функціонування СОДТ та/або КСЗІ (ЕФ); коефіцієнту старіння відомостей (КС); «питомої ваги» об'єкта відомостей та відносна вартість складової частини об'єкта (ПВОС); «питомої ваги» відомостей (СлІ/ДТ) та їх матеріальних носіїв інформації (ПВВН), що засновується на конкретних оцінках, які в результаті сформують значення показників W / $W_{iш}$, $W_{ін}$, $W_{ек}$, $K_{КСЗІ}^{\varphi}$ / $K_{СОДТ}^{\varphi}$, K_c , $Q(O^{\varphi})$, k, $W(L^{\varphi})/W(DS^{\varphi})$, $w(L_i^{PAs})/w(PV^{\varphi}{}_{N.i.j})$, $\beta^{PAs}(L_i^{PAs})/\beta^{\varphi}(PV^{\varphi}{}_{N.i.j})$, $\beta^{\varphi}(V(L_i^{PAs}))/\beta^{\varphi}(nL^{\varphi}(PV^{\varphi}{}_{N.i.j}))$, $\rho(L_i^{PAs})/\rho(nD^{\varphi})$, $\rho(V(L_i^{PAs}))/\rho(nL^{\varphi})$ і у подальшому їх буде використано для обчислення сукупних наслідків (шкоди, збитків) φ-го ОКІ.

БФКОКІІ – складається з модулів оцінювання та вибору параметрів і характеристик ОКІ, його ОКІІ (сектор критичної інфраструктури (СКІ); адміністративно-територіальна одиниця (АТО); форма власності (ФВ); назва або/та унікальний ідентифікаційний номер юридичної особи в Єдиному державному реєстрі підприємств та організацій України (ЄДРПОУ) організацій-власників/розпорядників системи як ОКІІ (УНН); видів інформації, що обробляється в системі (ВІ); номер документа, що засвідчує наявність атестованих/ліцензованих систем чи засобів захисту інформації (НДЗ); негативні наслідки кібератак на систему (НН); геолокаційний (та/або мережевий) ресурс ідентифікації ОКІ (ГР); формувач класифікатора об'єктів (ФКО), що засновується на конкретних параметрах діяльності ОКІ, які в результаті сформують значення показників ID у класифікатор ОКІІ як SS–UU–O–NN…N–RR…R–II–CC–MM, який у подальшому буде використано при формування реєстру порушень у модулі експертного висновку щодо наслідків (шкоди, збитків) φ-го ОКІ.

БОЕДу – складається блоку БОЕД у якому модуль ВР удосконалено за рахунок можливості обробки бального параметра оцінки ризику захисту ПД в АС (Н) для формування висновку про стан рівня захищеності ПД в конкретній АС та надання рекомендації (І) щодо підвищення цього стану шляхом запровадження відповідної політики безпеки та/або необхідних способів (методів) захисту інформації.

Детальний опис і склад блоку БФЕІ у [14]. Система та її режими роботи у підсистемах функціонують наступним чином. В БІКІ призначений для виконання функції нечіткої ідентифікації і класифікації інформації до відкритої або ІзОД $I = \langle PI, RI \rangle$ за такими її видами як ПД, СлІ, ДТ $RI = \langle CI, OI, IS \rangle$ (див. (1), (2) в [16, 17]), у т.ч. з використанням модулю ВВМ. Дана функція застосовується за наявністю запиту на виконання процедури щодо визначення підстав для віднесення відомостей до класифікованої ІзОД чи при експертизі матеріальних носіїв інформації на предмет наявності певного виду ІзОД шляхом отримання експертного висновку про наявність (відсутності) потенційної та/або істотної шкоди (збитків) у разі їх витоку з метою подальшого обмеження (вільного) доступу до них.

В БФКОКІІ встановлюються значення параметрів кортежу $ID = <ID_1, ID_2, ID_3, ID_4, ID_5, ID_6, ID_7, ID_8>$ в модулях СКІ, АТО, ФВ, УНН, ВІ, НДЗ, НН, АЛС, ФКО для формування у класифікатора ОКІІ як SS–UU–O–NN…N–RR…R–II–CC–MM, який буде використано при формування реєстру порушень у модулі експертного висновку щодо наслідків (шкоди, збитків) ПД, СлІ, ДТ φ-го ОКІ.

Принцип роботи підсистеми оцінювання наслідків витоку ПД. Якщо в БІКІ $RI = \langle CI \rangle$ та/або в БФЗДу(ПД) експерти відповідної предметної галузі або уповноважені особи формують запит (як CI) відповідно до вимог національного законодавства [30, 31] (далі – Режим 1) або n-компонентний експертний запит (як $\mathrm{IDF_i}\ (i = \overline{1,n})$) за вимогами GDPR [29] (далі – Режим 2), тоді працює підсистема оцінювання наслідків витоку ПД.

Режим 1. Модуль НКІ як $RI = \langle CI \rangle$ та/або фахівці відповідної предметної галузі формують в БФЗДу(ПД) в модулі БДГПХ експертний запит CI = <A, B, C, D, E, F, G, H, I>, що оцінює ризики витоку ПД, їхні характеристики та величину завданих збитків (шкоди), який поступає до БОНППД на вхід модулів ХПД, СО, АМБ, ХПБ, МО, ІЗ, ВЗ, ОР та КР. В цих модулях на основі отриманих вхідних величин розраховується значення показників K_{vd}, K_{vp}, K_m, C_n, R_{C_corr}, P_{riv_zag}, R_{max}, $R_{zag_{corr}}$, $I \in (I_{min}, I_{max})$ та $G \in (G_{min}, G_{max})$ (див. (3)-(13) в [8]) для подальшого їх використання БОЕДу. Далі у модулі ОРЗ здійснюється розрахунок бальної величини оцінки ризику захисту ПД Н та її вартісного (грошового) значення збитків (Rg), завданих від їх витоку. В удосконаленому модулі ВР за значенням Н (від 1 до 5 балів) формуються рекомендації (І) щодо варіантів застосування рекомендованої політики безпеки для досягнення необхідного рівня захищеності ПД в АС, які у подальшому заносяться до БДРВ для формування експертного висновку про оцінювання наслідків (шкоди, збитків) витоку ПД.

Режим 2. Детальний опис функціонування підсистеми оцінювання негативних наслідків витоку ПД, основаної на теоретико-множинній GDPR-моделі параметрів ПД [12], за n-компонентним експертним запитом $\mathrm{IDF_i}\ (i = \overline{1,n})$, процесу оцінювання параметрів цієї моделі, формування експертного висновку та рекомендацій RE^{φ} приведено в [14].

Принцип роботи підсистеми оцінювання наслідків витоку СлІ та/або ДТ.

Якщо у БІКІ $RI = \langle OI \rangle$ та/або у БЗДФВРП(СлІ/ДТ) державний експерт з питань таємниць та/або комісія з питань роботи зі СлІ, інші уповноважені особи) формують відповідно вимог національного законодавства запит (як OI) (далі – Режим 3) або у БІКІ $RI = \langle IS \rangle$ та/або у БЗДФВРП(СлІ/ДТ) сформовано запит (як IS) [30, 32] (далі – Режим 4), тоді працює підсистема оцінювання наслідків витоку СлІ та/або ДТ.

Режим 3. Модуль НКІ як $RI = \langle OI \rangle$ та/або комісія про роботі зі СлІ (уповноважена особа) формують в БЗДФВРП(СлІ/ДТ) в модулі БДГПХ експертний запит $OI = \langle OI_1, OI_2, OI_3, OI_4, OI_5, OI_6 \rangle$, що ідентифікує і оцінює параметри наявності СлІ за відповідним ПСлІ ОКІ, виконання вимог застосування «трискладового тесту», наявності базових параметрів можливої шкоди (по типу процедури первинного віднесення відомостей до IS), причинно-наслідкові і просторово-часові характеристик та ознаки для СлІ, ідентифікаторів (грифів/відміток), що використовуються для обмеження доступу до СлІ тощо, який поступає до БОПСлІ на вхід модулів МІ, ТТ, МЕ, МП, СОД, Г/В для сформування значення показників L, R, T_i^e, DR^l, $P_{\tau_f}^l$, V (див. (3)-(12) в [17]). Далі на основі отриманих значень в БОПШ визначаються необхідні параметри оцінювання потенційної істотної шкоди показників $W_{іш}$, $W_{ін}$, $W_{ек}$, $K_{КСЗІ}^{\varphi}$, K_c, $Q(O^{\varphi})$, k, $W(L^{\varphi})$, $w(L_i^{PAs})$, $\beta^{PAs}(L_i^{PAs})$, $\beta^{\varphi}(V(L_i^{PAs}))$, $\rho(L_i^{PAs})$, $\rho(V(L_i^{PAs}))$ (див. (1)-(72) в [24]) для подальшого їх зберігання у БДРОР, БДВРП і використання БЗДФВРП(СлІ/ДТ) при формуванні експертного висновку.

Режим 4. Модуль НКІ як $RI = \langle IS \rangle$ та/або комісія про роботі зі СлІ (уповноважена особа) формують в БЗДФВРП(СлІ/ДТ) в модулі БДГПХ експертний запит $IS = \langle IS_1, IS_2, IS_3, IS_4, IS_5, IS_6, IS_7, IS_8, IS_9 \rangle$, що ідентифікує наявність ДТ і оцінює первинні (див. (1)-(18) в [13]), внутрішні (див. (1)-(24) в [19, 20]) і вторинні (див. (1)-(26) в [21, 22]) параметри N^{φ}, A^{φ}, CD^{φ}, O^{φ}, SU^{φ}, CO^{φ}, CU^{φ}, DS^{φ}, P^{φ}, AP^{φ}, SD^{φ}, E^{φ}, RS^{φ}, NA^{φ}, FP^{φ}, nE^{φ}, nP^{φ}, FA^{φ}, nPN^{φ}, nA^{φ}, nSA^{φ}, nRA^{φ}, nWR^{φ}, nGA^{φ}, nWA^{φ}, SS^{φ}, aM^{φ}, nsM^{φ}, nrM^{φ}, nMr^{φ}, nMt^{φ}, nMf^{φ}, sU^{φ}, nMu^{φ}, tW^{φ}, SW^{φ}, nSW^{φ}, pSW^{φ}, tP^{φ}, SP^{φ}, nSP^{φ}, pSP^{φ}, nRR^{φ}, nCO^{φ}, nCS^{φ}, nD^{φ}, nL^{φ}, nDL^{φ}, nRD^{φ}, nDR^{φ}, nFA^{φ}, nFT^{φ} стану ефективності ОДТ в модулях СЗ, РСО, ДДП, МНСІ, ВСРВ, ЗСРВ, РПО, ФВР, МС, які основуються на конкретних оцінках діяльності ОКІ і в БОПШ сформують значення показників W, $W_{ін}$, $W_{ек}$, $K_{СОДТ}^{\varphi}$, K_c, $Q(O^{\varphi})$, k, $W(DS^{\varphi})$, $w(PV^{\varphi}{}_{N.i.j})$, $\beta^{\varphi}(PV^{\varphi}{}_{N.i.j})$, $\beta^{\varphi}(nL^{\varphi}(PV^{\varphi}{}_{N.i.j}))$, $\rho(nD^{\varphi})$, $\rho(nL^{\varphi})$ для подальшого їх зберігання у БДРОР, БДВРП і використання БЗДФВРП(СлІ/ДТ) при формуванні експертного висновку.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Розроблена структурна модель системи оцінювання наслідків (шкоди, збитків) у разі витоку таких видів ІзОД як ПД, СлІ, ДТ є необхідним інструментом для підвищення рівня інформаційної безпеки ОКІ, ефективності застосування систем захисту ІзОД (КСЗІ, СОДТ) та якості організації режиму секретності.

Запропонована система призначена для використання як ОКІ, так і державним експертом з питань таємниць, судово-експертними установами, комісією по роботі зі службовою інформацією, іншими уповноваженими особами тощо для оцінювання величини потенційної істотної або сукупної шкоди, шкоди від інших тяжких наслідків, інших завданих збитків від витоку кожного з цих видів ІзОД, що дозволить виявляти, аналізувати та прогнозувати потенційні ризики, пов'язані з втратою їх конфіденційності, з метою своєчасної мінімізації та ліквідації цих наслідків, необхідної для забезпечення стійкого та безперервного функціонування ОКІ для надання ним ОП/ЖВФ відповідно до вимог законодавства і стандартів інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бобро Д., та ін. (2019). Організаційні та правові аспекти забезпечення безпеки і стійкості критичної інфраструктури України. *Аналіт. доп.*, 224.
2. Єрменчук, О. (2018). Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України. *Монографія*, 180.
3. Kondratov, S., et al. (2017). Developing The Critical Infrastructure Protection System in Ukraine. *Monografia*, 184.
4. Falchenko, S., et al. (2020). Method of Fuzzy Classification of Information with Limited Access. *IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT)*, 255–259. https://doi.org/10.1109/ATIT50783.2020.9349358
5. Касперський, І. (2014). Класифікаційні ознаки службової інформації. *Інформаційна безпека людини, суспільства, держави, 3*(16), 104–109.
6. Архипов, О., & Муратов, О. (2011). *Критерії визначення можливої шкоди національній безпеці України у разі розголошення інформації, що охороняється державою*. Монографія.
7. Корченко, О., та ін. (2014). *Оцінювання шкоди національній безпеці України у разі витоку державної таємниці.* Монографія. https://www.researchgate.net/publication/388763890
8. Корченко, О., та ін. (2016). Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах, *Захист інформації*, *18*(1), 39-47. https://doi.org/10.18372/2410-7840.18.10111
9. Корченко, О., та ін. (2017). Ukrainian critical information infrastructure: terms, sectors and consequences. *Захист інформації*, *19*(4), 303-309. https://doi.org/10.18372/2410-7840.19.12220
10. Корченко, О., та ін. (2018). Модель класифікатора об'єктів критичної інформаційної інфраструктури держави. *Захист інформації*, *20*(1), 5-11. https://doi.org/10.18372/2410-7840.20.12448
11. Корченко, О., та ін. (2018). Модель оцінювання наслідків витоку державної таємниці від кібератак на критичну інформаційну інфраструктуру держави. *Безпека інформації*, *24*(1), 29-35. https://doi.org/10.18372/2225-5036.24.12606
12. Корченко, О., та ін. (2020). Теоретико-множинна GDPR-модель параметрів персональних даних. *Захист інформації*, *22*(2), 120-141. https://doi.org/10.18372/2410-7840.22.14871
13. Корченко, О., & Дрейс, Ю. (2022). Кортежна модель формування бази даних первинних параметрів для оцінювання стану охорони державної таємниці. *Безпека інформації*, 28 (1), 35-42. https://doi.org/10.18372/2225-5036.28.16911
14. Корченко, О., & Лозова І. (2024). Структурна модель системи оцінки негативних наслідків втрати персональних даних. *Наукові записки ДУІКТ*, *2*(6), 165-170. https://doi.org/10.31673/2786-8362.2024.028264
15. Дрейс, Ю. (2013). Метод нечіткої класифікації відомостей, що становлять державну таємницю за визначеними критеріями. *Вісник Національного університету «Львівська політехніка». Автоматика, вимірювання та керування*, 774, 10–16. https://www.researchgate.net/publication/405186418
16. Dreis, Yu., et al. (2022). Restricted Information Identification Model. *CEUR Workshop Proceedings, vol.3288*, 89-95. https://www.researchgate.net/publication/371657347
17. Дрейс, Ю. (2024). Модель параметрів оцінювання наслідків витоку службової інформації об'єкта критичної інфраструктури. *Кібербезпека: освіта, наука, техніка*, *2*(26), 200–211. https://doi.org/10.28925/2663-4023.2024.26.691
18. Дрейс, Ю. (2024). Метод оцінювання наслідків втрати об'єкта критичної інфраструктури за узагальненими критеріями. *Кібербезпека: освіта, наука, техніка*, *1*(25), 487–504. https://doi.org/10.28925/2663-4023.2024.25.487504
19. Dreis, Yu., et al. (2024). Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection. *CEUR Workshop Proceedings*, *vol.3654*, 277-289. https://www.researchgate.net/publication/379153460
20. Дрейс, Ю. (2025). Модель внутрішніх параметрів оцінювання стану охорони державної таємниці. *Захист інформації*, 27(1), 4-14. https://doi.org/10.18372/2410-7840.27.21170
21. Dreis Yu., et al. (2024). Model to Formation Data Base of Secondary Parameters for Assessing Status of the State Secret Protection. *CEUR Workshop Proceedings, vol.3800*, 1-11. https://www.researchgate.net/publication/385825539
22. Дрейс, Ю. (2025). Модель вторинних параметрів оцінювання стану охорони державної таємниці. *Захист інформації*, *27*(2), 68-78. https://doi.org/10.18372/2410-7840.27.21180

23. Дрейс, Ю. (2025). Удосконалений метод оцінювання шкоди національній безпеці України у разі витоку державної таємниці. *Кібербезпека: освіта, наука, техніка*, 3 (27), 489–521. https://doi.org/10.28925/2663-4023.2025.27.771
24. Дрейс, Ю. (2025). Метод оцінювання шкоди у разі витоку службової інформації. *Безпека інформації*, 31(3), 190-206. https://doi.org/10.18372/2225-5036.31.21166
25. Deineka O., et al. (2025). Detection confidential information by large language models. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska,* 15(3), 91–99. https://doi.org/10.35784/iapgos.6910
26. Mykhailyshyn, K., et al. (2025). Analysis of modern tools, methods of audit and monitoring of database security. *Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska*, 15(4), 124–129. https://doi.org/10.35784/iapgos.6993
27. Rzaieva, S., et al. (2025). Methods of personal data protection in retail: Practical solutions. *CEUR Workshop Proceedings*, *vol.*3991, 492–506. https://www.researchgate.net/publication/394929279
28. Слюсар, В. (2024). Локальні великі мовні моделі для обробки конфіденційної інформації. *Озброєння та військова техніка*, *44*(4), 79–91. https://slyusar.kiev.ua/OVT_04_24_Slyusar_m.pdf
29. *Про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільне переміщення таких даних*. Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27.04.2016. Переклад українською мовою. https://zakon.rada.gov.ua/laws/show/984_008-16
30. *Про доступ до публічної інформації*. Закон України № 2939-VI від 13.01.2011 (редакція від 08.08.2025). https://zakon.rada.gov.ua/laws/show/2939-17
31. *Про захист персональних даних.* Закон України № 2297-VI від 01.06.2010 (редакція від 14.05.2025). https://zakon.rada.gov.ua/laws/show/2297-17#Text
32. *Про державну таємницю*. Закон України № 3855-XII від 21.01.1994 (редакція від 27.08.2025). https://zakon.rada.gov.ua/laws/show/3855-12#Text
33. (Law No. 3855-XII, as amended August 27, 2025). https://zakon.rada.gov.ua/laws/show/3855-12

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

Yurii Dreis
PhD in Eng. (Information security of the State), Associate Professor
Associate Professor of System Analysis & Information Technologies Academic Department
Mariupol State University, Kyiv, Ukraine
ORCID: 0000-0003-2699-1597
y.dreis@mu.edu.ua

STRUCTURAL MODEL OF THE LIMITED-ACCESS INFORMATION LEAKAGE CONSEQUENCES ASSESSMENT SYSTEM

Abstract. The article presents a structural model of a system for evaluating the consequences of restricted information leaks, aimed at increasing the level of information security for individuals, society, and the state. The system allows for the automation of the following processes: identification and classification of public (open) information and restricted information; risk analysis with forecasting of potential consequences (harm, damage) from a possible or already occurred leak of personal data, official information, or state secrets (and/or the loss of their physical carriers), while minimizing financial losses and/or other severe consequences; and the formation of a violation registry and a critical information infrastructure object classifier. In accordance with the existing requirements regarding the specific organization of secrecy regimes and access to certain types of classified information, the developed system structure includes a subsystem for evaluating the consequences of personal data leaks (under national and international legislation, including GDPR) and a subsystem for evaluating the consequences of official information and/or state secret leaks. The proposed system ensures the evaluation of the operational effectiveness of information protection systems (comprehensive information protection systems and/or state secret protection systems) of critical infrastructure objects, government authorities, and secret-regime entities, and is intended for use by state experts on secrets, forensic institutions, commissions on official information, and other authorized persons.

Keywords: information protection; restricted information; consequence assessment (harm, damage); personal data; official information; state secret; risks; critical infrastructure object; model; decision support system; information leak.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Bobro, D., et al. (2019). Organizational and legal aspects of ensuring security and resilience of Ukraine's critical infrastructure. Analytical report.
2. Yermenchuk, O. (2018). Main approaches to organizing critical infrastructure protection in European countries: Experience for Ukraine. Monograph.
3. Kondratov, S., et al. (2017). Developing the critical infrastructure protection system in Ukraine. Monografia.
4. Falchenko, S., et al. (2020). Method of fuzzy classification of information with limited access. In 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (ATIT) (pp. 255-259). IEEE. https://doi.org/10.1109/ATIT50783.2020.9349358
5. Kasperskyi, I. (2014). Classification features of official information. Information Security of Person, Society and State, 3(16), 104-109.
6. Arkhypov, O., & Muratov, O. (2011). Criteria for determining possible damage to the national security of Ukraine in case of disclosure of state-protected information. Monograph.
7. Korchenko, O., et al. (2014). Assessment of damage to the national security of Ukraine in case of leakage of state secrets. Monograph. https://www.researchgate.net/publication/388763890
8. Korchenko, O., et al. (2016). Model and method for risk assessment of personal data protection during processing in automated systems. Information Protection, 18(1), 39-47. https://doi.org/10.18372/2410-7840.18.10111
9. Korchenko, O., et al. (2017). Ukrainian critical information infrastructure: Terms, sectors and consequences. Information Protection, 19(4), 303-309. https://doi.org/10.18372/2410-7840.19.12220
10. Korchenko, O., et al. (2018). Model of a classifier for state critical information infrastructure objects. Information Protection, 20(1), 5-11. https://doi.org/10.18372/2410-7840.20.12448
11. Korchenko, O., et al. (2018). Model for assessing consequences of state secret leakage caused by cyberattacks on critical information infrastructure. Information Security, 24(1), 29-35. https://doi.org/10.18372/2225-5036.24.12606

12. Korchenko, O., et al. (2020). Set-theoretic GDPR model of personal data parameters. Information Protection, 22(2), 120-141. https://doi.org/10.18372/2410-7840.22.14871
13. Korchenko, O., & Dreis, Y. (2022). Tuple model for forming a database of primary parameters for assessing the state secret protection status. Information Security, 28(1), 35-42. https://doi.org/10.18372/2225-5036.28.16911
14. Korchenko, O., & Lozova, I. (2024). Structural model of a system for assessing negative consequences of personal data loss. Scientific Notes of the State University of Information and Communication Technologies, 2(6), 165-170. https://doi.org/10.31673/2786-8362.2024.028264
15. Dreis, Y. (2013). Method of fuzzy classification of information constituting state secrets according to defined criteria. Bulletin of Lviv Polytechnic National University. Automation, Measurement and Control, 774, 10-16. https://www.researchgate.net/publication/405186418
16. Dreis, Y., et al. (2022). Restricted information identification model. CEUR Workshop Proceedings, 3288, 89-95. https://www.researchgate.net/publication/371657347
17. Dreis, Y. (2024). Model of parameters for assessing consequences of official information leakage at a critical infrastructure facility. Cybersecurity: Education, Science, Technique, 2(26), 200-211. https://doi.org/10.28925/2663-4023.2024.26.691
18. Dreis, Y. (2024). Method for assessing consequences of critical infrastructure object loss using generalized criteria. Cybersecurity: Education, Science, Technique, 1(25), 487-504. https://doi.org/10.28925/2663-4023.2024.25.487504
19. Dreis, Y., et al. (2024). Model to formation data base of internal parameters for assessing the status of the state secret protection. CEUR Workshop Proceedings, 3654, 277-289. https://www.researchgate.net/publication/379153460
20. Dreis, Y. (2025). Model of internal parameters for assessing the state secret protection status. Information Protection, 27(1), 4-14. https://doi.org/10.18372/2410-7840.27.21170
21. Dreis, Y., et al. (2024). Model to formation data base of secondary parameters for assessing status of the state secret protection. CEUR Workshop Proceedings, 3800, 1-11. https://www.researchgate.net/publication/385825539
22. Dreis, Y. (2025). Model of secondary parameters for assessing the state secret protection status. Information Protection, 27(2), 68-78. https://doi.org/10.18372/2410-7840.27.21180
23. Dreis, Y. (2025). Improved method for assessing damage to the national security of Ukraine in the event of state secret leakage. Cybersecurity: Education, Science, Technique, 3(27), 489-521. https://doi.org/10.28925/2663-4023.2025.27.771
24. Dreis, Y. (2025). Method for assessing damage caused by leakage of official information. Information Security, 31(3), 190-206. https://doi.org/10.18372/2225-5036.31.21166
25. Deineka, O., et al. (2025). Detection confidential information by large language models. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15(3), 91-99. https://doi.org/10.35784/iapgos.6910
26. Mykhailyshyn, K., et al. (2025). Analysis of modern tools and methods of audit and monitoring of database security. Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 15(4), 124-129. https://doi.org/10.35784/iapgos.6993
27. Rzaieva, S., et al. (2025). Methods of personal data protection in retail: Practical solutions. CEUR Workshop Proceedings, 3991, 492-506. https://www.researchgate.net/publication/394929279
28. Slyusar, V. (2024). Local large language models for processing confidential information. Weapons and Military Equipment, 44(4), 79-91. https://slyusar.kiev.ua/OVT_04_24_Slyusar_m.pdf
29. European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). https://zakon.rada.gov.ua/laws/show/984_008-16
30. Verkhovna Rada of Ukraine. (2011). On access to public information (Law No. 2939-VI, as amended August 8, 2025). https://zakon.rada.gov.ua/laws/show/2939-17
31. Verkhovna Rada of Ukraine. (2010). On personal data protection (Law No. 2297-VI, as amended May 14, 2025). https://zakon.rada.gov.ua/laws/show/2297-17
32. Verkhovna Rada of Ukraine. (1994). On state secrets (Law No. 3855-XII, as amended August 27, 2025). https://zakon.rada.gov.ua/laws/show/3855-12

Отримано редакцією журналу / Received: 28.02.26
Прорецензовано / Revised: 03.03.26
Схвалено до друку / Accepted: 25.06.26