УДК 004.056.53:004.7 DOI: 10.31673/2409-7292.2026.029318

Яцев Андрій Васильович
аспірант кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
E-mail: andrii.yatsev.asp.2025@lpnu.ua

Журавель Ігор Михайлович
доктор технічних наук, старший науковий співробітник, завідувач кафедри безпеки інформаційних технологій
Національний університет «Львівська політехніка», Львів, Україна
ORCID: 0000-0003-1114-0124
E-mail: ihor.m.zhuravel@lpnu.ua

МЕТОД КОМПЛЕКСНОГО ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ ЗНЕШКОДЖЕННЯ ТА РЕКОНСТРУКЦІЇ КОНТЕНТУ У МЕРЕЖЕВІЙ ІНФРАСТРУКТУРІ

У статті досліджено можливості застосування технології знешкодження та реконструкції контенту (Content Disarm and Reconstruction, CDR) для підвищення ефективності захисту мережевих ресурсів під час обробки та передачі файлів різних форматів. Актуальність дослідження зумовлена стрімким посиленням небезпек пов'язаних зі зростанням кількості прихованих загроз, що реалізуються через легітимні файлові структури та здатні обходити традиційні засоби виявлення шкідливого вмісту, що спричиняє високий рівень складності їх запобіганню або знешкодженню. Основну увагу зосереджено на розробці методу комплексної експериментальної оцінки ефективності застосування CDR-рішень як засобу превентивної протидії загрозам, що виникають під час обміну файлами з потенційно шкідливим вмістом. У межах роботи розглянуто основи проблеми безпеки контенту та ідею його очищення, як один з способів його вирішення, а також принцип дії технології знешкодження та реконструкції контенту, який полягає у видаленні активних та потенційно небезпечних елементів файлу з подальшим формуванням його безпечної копії на основі стандартної структури відповідного файлового формату, що піддавався обробці. Проаналізовано особливості застосування CDR до різних типів файлів, зокрема документів, архівів, зображень та мультимедійного контенту, а також визначено її переваги порівняно з класичними сигнатурними та поведінковими засобами захисту, такими як антивіруси та методи виявлення в пісочниці. Запропоновано експериментальну методику масового тестування CDR-рішень на великих обсягах файлів із подальшим аналізом результатів та формуванням системи кількісних показників ефективності, що враховують рівень знешкодження прихованих загроз, коректність реконструкції, продуктивність обробки та вплив на мережеві й обчислювальні ресурси. У підсумку визначено напрями подальших досліджень, зокрема уточнення оптимальних сценаріїв застосування технології знешкодження та реконструкції контенту, формалізацію критеріїв ефективності та розробку методів оптимізації продуктивності при збереженні високої якості реконструкції файлів.

Ключові слова: кібербезпека; захист інформації; безпека мережі; content disarm.

Вступ

Сучасний стан інформаційних технологій та висока інтенсивність обміну інформацією шляхом її передавання мережевою інфраструктурою зумовлює ускладнення загроз інформаційної безпеки. Все більшого поширення зазнає використання звичних файлових структур для вбудовування в нього нестандартних елементів або стеганографічних вставок, що дозволяє обходити традиційні сигнатурні чи поведінкові засоби виявлення. У таких умовах, підходи, що орієнтуються на виявлення уже відомих ознак зловмисних дій, показують все нижчу ефективність, особливо до загроз нульового дня.

Як противага цим викликам все більше уваги викликають підходи, що реалізують методи превентивного захисту. Одним з таких є застосування технології знешкодження та реконструкції контенту. Головним засобом захисту у ній виступає попереднє знешкодження усіх активних та потенційно небезпечних елементів із подальшим відновленням інформації на основі стандартної структури файлу відповідного формату. Сучасні дослідження показують, що дана технологія має високу ефективність у попередженні можливих загроз та значні переваги над традиційними засобами захисту. Проте існує проблема об'єктивної оцінки ефективності CDR-рішень в реальних умовах мережевої інфраструктури. Відсутність

уніфікованих методів і кількісних показників ускладнює порівняльний аналіз різних рішень, а також обґрунтований вибір і оптимальне впровадження технології у системах захисту інформації. У зв'язку з цим актуальним є розроблення методу комплексної оцінки ефективності технології знешкодження та реконструкції контенту у мережевій інфраструктурі.

Постановка проблеми

Великі обсяги цифрової інформації, що циркулюють мережевою інфраструктурою, уже стали звичними у сучасному світі, проте це несе все нові та нові виклики безпеки. Використання вбудованих скриптів, стеганографічних вставок та різних модифікацій стандартної структури файлів дозволяє зловмисникам обійти класичні засоби захисту такі як антивірусний аналіз та виявлення у пісочниці. Звідси випливає висновок, що навіть при багаторівневій системі захисту, ризик компрометації мережевих ресурсів є високим.

Технологія знешкодження та реконструкції контенту постає як перспективний засіб попередньої обробки файлів, який ґрунтується не на виявленні шкідливих вставок, а на зміні самого вмісту об'єкту для повного знищення усіх потенційно небезпечних елементів та утворенням безпечної копії вхідного файлу.

Незважаючи на наявність теоретичних обґрунтувань і практичних реалізацій даної технології, все ж залишається невирішеною проблематика об'єктивної та відтворюваної оцінки їх ефективності в умовах реальної мережевої інфраструктури. Адже існуючі підходи до оцінювання технології знешкодження та реконструкції контенту зосереджені на обрахуванні показників успішного усунення шкідливих елементів у тестуваннях окремих зразків файлів. Водночас відсутні уніфіковані методи, які б комплексно оцінювали ефективність CDR з урахуванням рівня знешкодження прихованих загроз, коректності реконструкції файлів, продуктивності обробки, масштабованості, а також впливу на мережеві та обчислювальні ресурси.

Тому необхідним є розроблення методу оцінки ефективності застосування технології знешкодження та реконструкції контенту у мережевому середовищі, за допомогою якого можна було б здійснювати порівняльний аналіз різних CDR-рішень, а також визначати доцільність їх впровадження в конкретних сценаріях обміну файлами та формувати обґрунтовані вимоги до їх продуктивності й якості реконструкції. Розв'язання цієї проблеми є необхідною умовою для підвищення рівня захисту мережевих ресурсів в умовах зростання великої кількості прихованих загроз.

Аналіз останніх досліджень і публікацій

Питання безпеки контенту та попередження прихованих загроз все активніше досліджується. У дослідженнях [1] сформульовано базову постановку задачі захисту контенту шляхом його перетворень, де обґрунтовується рух від класичних підходів до засобів зміни вмісту з попереднім усуненням усіх потенційно небезпечних елементів. Розвиток цього підходу представлено в подальших роботах [2], де запропоновано класифікацію трансформацій контенту та визначено їх застосовність для протидії різним типам загроз.

У проведеному порівняльному аналізі стратегій захисту контенту [3], включно з сигнатурними, поведінковими та методами перетворень, показано переваги технології знешкодження та реконструкції контенту у попередженні з невідомих атак. Також у аналізі [4] використання стеганографії у шкідливих цілях підкреслюється обмеження традиційних засобів виявлення щодо прихованих каналів передачі.

Практичні аспекти впровадження CDR-технології розглянуті в галузевих звітах [5-7], де описано принципи роботи, критерії вибору та архітектурні особливості комерційних CDR-рішень. Спеціалізовані дослідження присвячені застосуванню даної технології до окремих типів контенту, зокрема зображень [8] та PDF-документів [9], що демонструє гнучкість технології щодо різних форматів файлів. Також CDR-технологія розглядається в контексті безпеки передачі файлів як обов'язковий метод очищення контенту [10] перед обміном

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318

даними, що підтверджує її ефективність у практичних сценаріях. Окрім цього досліджується інтеграція CDR із концепцією нульової довіри для захисту моделей штучного інтелекту [11], а також знешкодження атак у нейронних мережах [12].

Проблема прихованих загроз у мультимедійному контенті та моделях машинного навчання систематизована в огляді [13], який підкреслює актуальність методів перетворення вмісту файлів для протидії стеганографічним елементам. Методологічні аспекти оцінювання ефективності захисту від загроз нульового дня також розглянуті в сучасних дослідженнях [14], що є важливим для побудови експериментальних методик оцінки CDR-рішень.

Загалом проаналізовані джерела свідчать, що технологія знешкодження та реконструкції контенту є перспективним напрямом превентивного захисту, здатним ефективно доповнювати або замінювати класичні методи виявлення шкідливого контенту, особливо в умовах зростання кількості прихованих та невідомих загроз.

Мета статті

Метою даного дослідження є розробка методу комплексної оцінки ефективності застосування технології знешкодження та реконструкції контенту, а також аналіз її можливостей як основного елемента системи контролю даних для підвищення рівня захисту мережевих ресурсів.

Для досягнення поставленої мети у роботі визначено такі завдання: провести аналіз принципу дії технології знешкодження та реконструкції контенту та її застосування до різних типів файлів; здійснити порівняння CDR із класичними сигнатурними та поведінковими засобами захисту; сформувати систему кількісних показників ефективності; розробити метод комплексної експериментальної оцінки ефективності CDR-рішень; визначити напрями подальших досліджень.

Проблема безпеки контенту

Масовий обмін цифровим контентом призвів до того, що стандартні типи файлів, такі як документи, зображення, архіви тощо, через свою необхідність у використанні для забезпечення процесів інформаційних систем стали носіями загроз, що можуть мати критичний вплив на мережеві ресурси. Системам захисту надзвичайно складно протидіяти атакам, що реалізуються шляхом приховування у стандартні формати та не містять явних ознак шкідливості. Як показують дослідження у сфері безпеки контенту, значна частина сучасних загроз маскується саме таким чином, що суттєво ускладнює їх ідентифікацію звичними засобами аналізу та виявлення [1, 3].

Сигнатурні антивірусні системи та методи поведінкового виявлення у пісочниці спрямовані на протидію атакам, шаблони чи ознаки яких уже відомі на момент опрацювання. Їх принцип дії спрямований саме на пошук ознак та аналіз виконуваного коду, проте такий підхід є надто вразливим до загроз нульового дня, а також є малоефективні до цільових модифікацій файлів і багатоступеневим атакам, які активуються лише за специфічних умов [3, 14].

Також загрози безпеці контенту несе активне використання стеганографії, що робить можливим приховування коду у зображеннях, мультимедійному вмісті тощо. Адже при такому сценарії атаки шкідливі елементи не проявляють себе на етапі аналізу поведінки та робить традиційні засоби неефективними [4, 13].

Як відповідь на дані виклики сформувалась концепція безпеки контенту шляхом його перетворень, яка передбачає, що потрібно не виявляти потенційно небезпечні вставки у файлах, а превентивно знешкоджувати завдяки контрольованим трансформаціям контенту. Даний підхід зміщує фокус з реактивного виявлення загроз на їх повне превентивне усунення незалежно від їх новизни та складності. У межах даної концепції файл розглядається не як об’єкт, що потребує перевірки, а структура, що повинна бути приведена до безпечного стану та лише у такому вигляді бути доставлена до кінцевого користувача [1, 2]. Основним технологічним втіленням даного підходу виступає технологія знешкодження та реконструкції

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318

контенту, яка полягає у детальному аналізі структури файлу, усуненні усіх активних та потенційно небезпечних компонентів з нього та відтворенні безпечної копії файлу відповідно до початкового формату.

Дана технологія зберігає незалежність від сигнатур та не має потреби у точній ідентифікації загрози, що робить її потенційно надефективною до прихованих загроз у контенті. Сучасні дослідження висувають рекомендації щодо імплементації технології та аналітичні огляди підкреслюють доцільність використання CDR як обов'язкового елемента сучасних систем захисту інформації, особливо в умовах високої інтенсивності файлового трафіку та складних ланцюгів обміну даними [1,3,5-9].

Останні наукові роботи демонструють подальше розширення сфери застосування технології знешкодження та реконструкції контенту за межі класичної файлової безпеки, зокрема, технологія інтегрується з архітектурними підходами нульової довіри. Дослідження у сфері безпеки передачі файлів також підтверджують ефективність CDR як обов'язкового етапу очищення контенту перед його обробкою, зберіганням або передачею в мережеву інфраструктуру [10-12].

Таким чином, сучасна проблема безпеки цифрового контенту зумовлена стрімким зростанням кількості прихованих та все нових невідомих загроз, для протидії яким традиційні механізми захисту не є достатньо ефективними. У цих умовах CDR-технологія постає не як допоміжний інструмент, а як ключовий елемент сучасної системи безпеки контенту, що забезпечує превентивний захист мережевих ресурсів незалежно від типу файлів та рівня розвитку загроз інформаційної безпеки.

Аналіз архітектури та методів CDR-технології

В основі рішень CDR лежить простий принцип дії (рис. 1), що полягає в аналізі прийнятого файлу, виділення корисної інформації, видаленні усіх «активних» та потенційно небезпечних вставок, та подальше відтворення цілком безпечної копії файлу, яка зберігає його формат, смислове навантаження та цінні дані.

Таким чином дана технологія усуває загрози, що пов'язані з безпекою файлів, адже поширення небезпечного вмісту, який замасковано у цілком легітимний контент, під час передавання даних мережею є одним з головних викликів сучасної безпеки. Головною небезпекою є те, що зловмисники здатні приховати шкідливі вставки у звичні формати файлів, які не здатні самі нести загрозу, і таким чином значно ускладнює їх виявлення класичними спеціалізованими засобами [5-9].

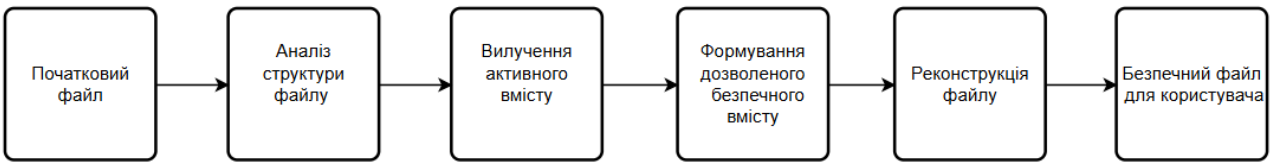

Рис. 1. Загальний принцип дії CDR-технології [5-9]

Відкриття файлу, що має в собі потенційно небезпечний вміст може нести за собою запуск зловмисних команд, які нанесуть шкоду мережевій інфраструктурі. І головним недоліком звичних засобів виявлення, таких як антивіруси, є те, що вони допускають загрозу нульового дня, тобто здатні виявити загрозу лише після її активності. Адже класична перевірка файлів полягала у двох засобах – антивірусному виявленні та аналізі у пісочниці. Обидва підходи полягають у факті виявлення зловмисного коду, в той час як CDR реалізує підхід нульової довіри, працюючи з файловим форматом та усуває усі потенційно небезпечні елементи.

Основні відмінності між технологією знешкодження та реконструкції контенту подано у таблиці 1 [3, 5-9].

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318

Таблиця 1

Головні відмінності традиційних засобів перевірки файлів та CDR [3, 5-9]

Критерії для порівняння	**CDR**	**Антивіруси**	**Виявлення в пісочниці**
Головний принцип роботи	Видалення усього вмісту, що може нести загрозу та відтворення безпечної копії вихідного файлу	Сигнатурне або ж спрямоване на аналіз аномалій виявлення та знешкодження шкідливого коду	Ізоляція об'єктів у спеціальному середовищі для спостереження за їх поведінкою
На що орієнтується при виконанні роботи	На файл, його тип та стандартну структуру, що відповідає йому	На відповідність сигнатурам або на аномальну активність	На аналіз динамічної поведінки файлу у спеціальному середовищі
Залежність від сигнатур	Відсутня	Критична	Відсутня
Чи є потреба у визначенні шкідливості	Ні	Так	Так
Чи є здатність усувати загрози нульового дня	Так, є	Вкрай обмежена	Так, є
Тип реагування на можливу загрозу	Превентивне видалення усього активного вмісту, що може її нести	Блокування загрози, спроба її усунути	Аналіз загрози із подальшим блокуванням
Ризик хибних спрацювань	Відсутній	Можливий	Можливий з низькою ймовірністю
Рівень захисту від прихованих загроз у файлах	Дуже високий	Низький або ж середній	Високий
Можливий рівень негативного впливу на активні процеси	Низький, при коректному застосуванні файл одразу повинен бути готовим до вжитку після обробки	Високий, адже існує ймовірність повного блокування файлу чи не розпізнання загрози в ньому	Середній, існує ризик затримки можливості доступу до файлів, через потребу значного часу для його аналізу
Звичне місце використання	Поштові сервери, веб-шлюзи, файлові сервіси, кінцеві пристрої	Кінцеві пристрої	Поштові сервери, веб-шлюзи
Рівень протидії методам приховування та обходу	Високий	Посередній	Посередній
Можлива роль для застосування у моделі Zero Trust	Основний засіб попереднього контролю контенту	Допоміжний засіб захисту	Засіб для аналізу
Головний недолік	Ризик можливої не функціональності файлу після його обробки	Критично низька ефективність проти невідомих загроз	Затребуваність великих ресурсів та можливі затримки для використання файлу

Виходячи з цього, можна зробити висновок, що технологія знешкодження та реконструкції контенту може стати ключовим інструментом для знешкодження загроз щодо безпечної роботи з файлами. Слід зазначити, що успіх її використання залежна від розуміння конкретного файлового формату, що піддається обробці. Адже для CDR критично важливим є розуміння файлової структури та його складових, саме тоді існує можливість очищення файлу зі збереженням його подальшої функціональності [5-9]. Для детальнішого ознайомлення слід розглянути архітектуру CDR-рішення для обробки зображень формату JPEG (рис. 2) [8].

Рис. 2. Архітектура CDR для обробки зображень [8]

Зображення даного формату має чітку будову [15]. Файл складається з трьох основних частин, а саме заголовок, що містить інформацію про тип, розмір та власника, метадані, у яких вказується тип стиснення та роздільна здатність зображення, а також піксельні дані, що формують кольори зображення. CDR опрацьовує такий файл таким чином, що витягує RGB-дані та на їх основі формує нове зображення, вписуючи нові метадані.

Для знищення усіх вставок, що можуть нести небезпеку, технологія знешкодження та реконструкції контенту застосовує цілий ряд засобів. Перш за все, виконується зміна розміру зображення, найчастіше його стиснення, таким чином змінюється масштаб та дані кольору, усуваючи можливі стеганографічні вставки, проте зберігаючи структуру вихідного файл [8].

Другим застосовується накладання фільтрів, а саме різноманітні типи розмиття, зміна яскравості та контрастності, для спотворення початкових даних з метою усунення тих же стеганографічних елементів, що виявились стійкими до стиснення[8].

Таблиця 2

Таблиця показників ефективності CDR-рішень

Показник ефективності	Позначення	Опис показника	Одиниця виміру
Рівень знешкодження прихованих загроз	$E_{зн}$	Частка файлів, у яких потенційно небезпечні елементи успішно вилучено	%
Коректність реконструкції	$E_{рек}$	Частка файлів, що після обробки зберігають функціональну придатність	%
Продуктивність обробки	P_{cdr}	Середня кількість файлів, оброблених за одиницю часу	файлів/с
Пропускна здатність CDR	B_{cdr}	Середня кількість інформації оброблених за одиницю часу	МБ/с
Затримка обробки	$T_{затр}$	Середній час обробки одного файлу	с
Середній час обробки пакета файлів	$T_{с}$	Середній час обробки пакета файлів	с
Рівень втрати даних	$L_{дані}$	Частка інформації, втраченої внаслідок реконструкції	%
Відсоток помилкових відмов	$F_{помилка}$	Частка легітимних файлів, що не пройшли CDR	%
Повторюваність результатів	$R_{повт}$	Стійкість результатів при повторних тестах	%
Максимальна стабільна швидкість	S_{max}	Швидкість обробки, при якій не втрачається якість реконструкції	МБ/с
Відсоток повністю функціональних файлів	$Q_{п.ф.}$	Частка файлів, що після обробки зберігають повну функціональну придатність	%
Рівень спотворення контенту	$D_{к}$	Частка зниження візуальної/функціональної якості файлу	%
Загальна інтегральна ефективність	$E_{і}$	Узагальнений показник ефективності CDR-рішення	безрозмірний

Кінцевим засобом обробки файлу є транскодування, що полягає у перетворенні між форматами, для прикладу перепис JPEG-зображення у PNG-формат та подальше зворотне перетворення у JPEG. Таким чином змінюється структура файлу та утворюються значно важчі умови для ймовірної реалізації шкідливого коду. Слід відзначити, що технологія не модифікує

початковий файл, а внаслідок його аналізу створює повністю новий, що ґрунтується на ключових структурних даних вхідного [8].

Розробка методу комплексної оцінки ефективності

Задля успішного застосування технології знешкодження та реконструкції контенту в умовах роботи реальної мережевої інфраструктури потрібно розуміти критерії, за якими можна оцінити ефективність її роботи. Існуючі дослідження звертають уваги лише на успішність знешкодження загроз та схожість безпечної копії файлу до початкового, а також збереження функціональності файлу [8, 9]. Проте такий обмежений перелік критеріїв не дає повного розуміння успішності використання CDR-рішень.

Тому для розробки методу комплексної оцінки ефективності застосування технології знешкодження та реконструкції контенту слід визначити цілу низку критеріїв. Їх перелік, позначення, короткий опис та одиницю виміру підведено у таблиці 2.

Оскільки дані критерії мають різну розмірність, то для подальших розрахунків спершу потрібно провести нормалізацію часткових показників, яка полягає у приведенні початкових числових значень до інтервалу $[0; 1]$.

Для показників у яких більше їх значення означає більш оптимальний стан нормалізація відбувається методом максимізації:

$$x_i = \frac{x_i - x_i^{\min}}{x_i^{\max} - x_i^{\min}} . \quad (1)$$

Для показників у яких менше їх значення означає більш оптимальний стан нормалізація відбувається методом мінімізації:

$$x_i = \frac{x_i^{\max} - x_i}{x_i^{\max} - x_i^{\min}} . \quad (2)$$

Далі потрібно сформувати вектор нормалізованих значень для кожного CDR-рішення, що піддавалося тестуванню:

$$\mathrm{x} = (x_1, x_2, \dots, x_n), n = 12 . \quad (3)$$

Слід зазначити, що n – це кількість врахованих показників ефективності у даному методі.

Наступним кроком є розробка вагових коефіцієнтів показників, тому для означення різного ступеня важливості показників вводиться вектор ваг:

$$\mathrm{w} = (w_1, w_2, \dots, w_n) , \quad (4)$$

$$\sum_{i=1}^{n} w_i = 1, w_i > 0 . \quad (5)$$

Виходячи звідси, показник комплексної оцінки ефективності застосування технології знешкодження та реконструкції контенту обраховується як зважена сума нормалізованих показників:

$$E_{int} = \sum_{i=1}^{n} w_i \cdot x_i , \quad (6)$$

$$E_{int} \in [0; 1] . \quad (7)$$

Даний показник кількісно визначає ефективність використання CDR-рішення, що було піддано тестуванню, та чим він вищий, тим більш обґрунтованим та успішним є застосування даного рішення реалізації технології знешкодження та реконструкції контенту.

Також обрахування даного критерію дозволяє об’єктивно проводити порівняння CDR-рішень. Також виходячи з даного методу можна обраховувати часткові показники

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318

ефективності, з яких слід виділити безпекову та експлуатаційну компоненти, а також якість контенту.

$$E_{\text{безпека}} = w_i^{\text{безп.}} E_{\text{зн}} + w_i^{\text{безп.}} E_{\text{рек}} + w_i^{\text{безп.}} L_{\text{дані}} , \quad (8)$$

$$E_{\text{експл.}} = w_i^{\text{е}} P_{cdr} + w_i^{\text{е}} B_{cdr} + w_i^{\text{е}} T_{\text{затр}} + w_i^{\text{е}} T_c + w_i^{\text{е}} F_{\text{помилка}} + w_i^{\text{е}} R_{\text{повт}} + w_i^{\text{е}} S_{max} , \quad (9)$$

$$E_{\text{я.к.}} = w_i^{\text{я.к.}} Q_{\text{п.ф.}} + w_i^{\text{я.к.}} D_{\text{к}} . \quad (10)$$

Таким чином, згідно запропонованого методу, завдяки широкому підбору критеріїв можна обчислити не лише значення загальної ефективності застосування, а й часткові показники відповідно до критично важливих компонентів безпеки контенту та мережевого середовища.

Для демонстрації переваг пропонованого методу було використано програмний продукт, що реалізує принцип технології знешкодження та реконструкції контенту Dangerzone, а також набір зображень для тестування.

Оцінка якості зображень проводилась завдяки PSNR (Peak Signal-to-Noise Ratio), що оцінює рівень піксельних відмінностей між оригінальним та обробленим зображенням, SSIM (Structural Similarity Index) характеризує структурну подібність між зображеннями, враховуючи контраст, яскравість та текстуру та UQI (Universal Quality Index) інтегрує кореляцію, яскравість та контраст для оцінки загальної перцептивної якості зображення. За результатами обрахунків отримано такі усереднені значення: $PSNR = 24.5453\, dB$, $SSIM = 0.9661$, $UQI = 0.9491$

Отримані значення PSNR свідчать про наявність піксельної деградації зображення після обробки. Водночас високі показники SSIM та UQI підтверджують збереження структурної та перцептивної цілісності документа. Це вказує на відсутність критичних візуальних спотворень, незважаючи на зміни на рівні піксельного представлення.

Результати тестування подані у таблиці 3.

Таблиця 3

Таблиця значень ефективності CDR-рішень

Показник ефективності	Позначення	Значення	Одиниця виміру	Нормалізовані значення	Ваги для інтегрального показника
Рівень знешкодження прихованих загроз	$E_{\text{зн}}$	100	%	1	0,15
Коректність реконструкції	$E_{\text{рек}}$	100	%	1	0,12
Продуктивність обробки	P_{cdr}	1,2	файлів/с	0,6	0,06
Пропускна здатність CDR	B_{cdr}	0,07	МБ/с	0,7	0,05
Затримка обробки	$T_{\text{затр}}$	0,83	с	0,35	0,06
Середній час обробки пакета файлів	$T_{\text{с}}$	8,3	с	0,17	0,05
Рівень втрати даних	$L_{\text{дані}}$	0	%	1	0,12
Відсоток помилкових відмов	$F_{\text{помилка}}$	0	%	1	0,06
Повторюваність результатів	$R_{\text{повт}}$	100	%	1	0,1
Максимальна стабільна швидкість	S_{max}	0,07	МБ/с	0,7	0,05
Відсоток повністю функціональних файлів	$Q_{\text{п.ф.}}$	100	%	1	0,12
Рівень спотворення контенту	$D_{\text{к}}$	3,39	%	0,66	0,06

Ваговий розподіл для інтегрального показника ефективності проводився за нормальним розподілом із пріоритетом на безпеку, забезпечуючи більш високу оцінку для критично

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318

важливих елементів і мінімізацію ризику пропуску потенційних загроз, а для часткових компонент за рівномірним розподілом.

Значення інтегрального показника ефективності за пропонованим методом становить:

$$E_{int} = \sum_{i=1}^{n} w_i \cdot x_i = 0{,}978\ . \tag{11}$$

В той час як стандартний метод зводиться до обрахування лише безпекової компоненти:

$$E_{\text{безпека}} = 0{,}3333 \cdot 1 + 0{,}3333 \cdot 1 + 0{,}3333 \cdot 1 = 0{,}99\ . \tag{12}$$

Також важливою умовою ефективності є якість контенту. Обрахування даної компоненти:

$$E_{\text{я.к.}} = 0{,}5 \cdot 1 + 0{,}5 \cdot 0{,}661 = 0{,}5 + 0{,}3305 = 0{,}8305 \approx 0{,}83\ . \tag{13}$$

Обрахування експлуатаційної компоненти:

$$\begin{gathered} E_{\text{експл.}} = 0{,}14286 \cdot 0{,}60 + 0{,}14286 \cdot 0{,}70 + 0{,}14286 \cdot 0{,}917 + \\ 0{,}14286 \cdot 0{,}170 + 0{,}14286 \cdot 1 + 0{,}14286 \cdot 1 + 0{,}14286 \cdot 0{,}7 \approx\ 0{,}73\ . \end{gathered} \tag{14}$$

У підсумку, пропонований метод не лише уточнює показники ефективності застосування технології знешкодження та реконструкції контенту, а й забезпечує ширшу картину для глибшого розуміння її впливу та результатів.

Результати дослідження

Під час проведення дослідження розроблено метод комплексної оцінки ефективності застосування технології знешкодження та реконструкції контенту, що ґрунтується на поєднанні критеріїв безпеки, збереження функціональності та якості файлів, а також оцінки продуктивної спроможності обробки. Проведений аналіз принципу дії CDR-технології підтверджує, що даний підхід спроможний з однаковою успішністю усувати приховані загрози без необхідності їх попередньої ідентифікації у різноформатних файлах.

Виконане порівняння досліджуваної технології та традиційних сигнатурних і поведінкових засобів виявлення прихованого шкідливого вмісту свідчить, що технологія знешкодження та реконструкції контенту забезпечує вищий рівень стійкості до невідомих атак та загроз нульового дня, завдяки видаленню потенційно небезпечних елементів ще на етапі попередньої обробки файлів.

Також у ході дослідження сформовано систему кількісних показників, що дає змогу оцінити ефективність CDR-рішень за основними важливими напрямками її роботи, а розроблений метод комплексної експериментальної оцінки дозволяє отримувати узагальнену характеристику ефективності CDR-рішень та порівнювати їх між собою.

Отримані результати підтверджують доцільність використання технології знешкодження та реконструкції контенту як ключового елемента системи безпеки даних для підвищення рівня захисту мережевих ресурсів та формують основу для подальших досліджень, спрямованих на подальше тестування CDR-технології у реальних умовах мережевої інфраструктури та розробки оптимальної моделі її застосування у середовищах різної архітектурної будови, зокрема моделі нульової довіри.

Висновки та перспективи подальших досліджень

У статті обґрунтовано доцільність застосування технології знешкодження та реконструкції контенту як ефективного інструмента підвищення рівня захисту мережевих ресурсів під час обробки та передачі файлів різних форматів. Адже CDR-рішення дозволяють мінімізувати ризики поширення шкідливого вмісту завдяки превентивному видаленню потенційно небезпечних елементів, незалежно від наявності відомих сигнатур. Розроблений метод комплексної оцінки ефективності технології знешкодження та реконструкції контенту забезпечує формалізований підхід до аналізу їхніх характеристик і дає змогу враховувати не лише показники безпеки, а й збереження функціональності файлів та продуктивність обробки.

Порівняльний аналіз із традиційними сигнатурними та поведінковими засобами захисту підтвердив значні переваги CDR-технології у забезпеченні потрібного рівня безпеки під час

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318

роботи з файлами. Отримані результати свідчать, що інтеграція даної технології у системи контролю даних є перспективним напрямом розвитку сучасних систем захисту інформації.

Подальші дослідження доцільно зосередити на поглибленому аналізі ефективності технології знешкодження та реконструкції контенту в умовах реальних корпоративних середовищ, з урахуванням різних сценаріїв загроз та інтенсивності обміну даними.

Актуальним є дослідження впливу CDR-рішень на цілісність і коректність складних структурованих документів, зокрема файлів із вбудованими об’єктами, скриптами та мультимедійним контентом.

Перспективним напрямом є уточнення системи показників комплексної оцінки ефективності з метою підвищення її адаптивності до різних класів інформаційних систем, зокрема вимог та принципів моделі нульової довіри.

Також доцільним є дослідження можливостей поєднання CDR із іншими механізмами контролю даних і виявлення загроз у складі систем кіберзахисту, а також оцінювання масштабованості CDR-рішень у хмарних та розподілених інфраструктурах.

Перелік посилань

1. Wiseman, S. (2017). Content security through transformation: Problem statement (Report DS-2017-1). Deep Secure. DOI: 10.13140/RG.2.2.13179.92969.

2. Wiseman, S. (2018). Classes of content transform (Technical Report Deep Secure-2018-1). Deep Secure. DOI: 10.13140/RG.2.2.13130.47043.

3. Wiseman, S. (2017). Comparing content threat defence strategies. Deep Secure. DOI: 10.13140/RG. 2.2.27431.85925.

4. Wiseman, S. (2017). Stegware: Using steganography for malicious purposes (Report DS-2017-4). Deep Secure. DOI: 10.13140/RG.2.2.15283.53289.

5. OPSWAT. (n.d.). Content disarm and reconstruction (CDR) selection guide. OPSWAT. https://info.opswat. com/hubfs/Demand%20Gen%20Assets/White%20Papers/OPSWAT_CDR_SelectionGuide_EN.pdf.

6. OPSWAT. (2023). OPSWAT deep CDR: Content disarm and reconstruction. OPSWAT. https://selabs.uk/wp-content/uploads/2024/03/cdr-protection-enterprise-OPSWAT-Deep-CDR-2023-10.pdf.

7. Olzak, T. (2025). Content disarm and reconstruction (CDR). https://www.researchgate.net/profile/Tom-Olzak/publication/389551208_Content_Disarm_and_Reconstruction_CDR/links/67c734b7645ef274a49ab7eb/Content-Disarm-and-Reconstruction-CDR.pdf.

8. Belkind, E., Dubin, R., & Dvir, A. (n.d.). Open image content disarm and reconstruction. https://arxiv.org/ pdf/2307.14057.

9. Dubin, R. (n.d.). Content disarm and reconstruction of PDF files. DOI: 10.1109/ACCESS.2023.3267717.

10. Coelho, J. F. C. (n.d.). Segurança em transferências de arquivos: A importância da limpeza de arquivos na sua transferência através de uma tecnologia content disarm and reconstruction e a sua implementação. http://hdl.handle.net/10400.26/51138.

11. Gilkarov, D., & Dubin, R. (n.d.). Zero-trust artificial intelligence model security based on moving target defense and content disarm and reconstruction. https://arxiv.org/pdf/2503.01758.

12. Dubin, R. (n.d.). Disarming attacks inside neural network models. https://arxiv.org/pdf/2309.03071.

13. Chaganti, R., Ravi, V., Alazab, M., & Pham, T. D. (n.d.). Stegomalware: A systematic survey of malware hiding and detection in images, machine learning models and research challenges. https://arxiv.org/pdf/2110.02504

14. Berlin, K., & Saxe, J. (n.d.). Improving zero-day malware testing methodology using statistically significant time-lagged test samples. https://arxiv.org/pdf/1608.00669.

15. Hamilton, E. (1992). JPEG file interchange format. C-Cube Microsystems. https://www.w3.org/Graphics/ JPEG/jfif3.pdf.

Andrii Yatsev
Postgraduate student, Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
E-mail: andrii.yatsev.asp.2025@lpnu.ua

Ihor Zhuravel
Doctor of Technical Sciences, Senior Researcher, Head of the Department of Information Technology Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0003-1114-0124
E-mail: ihor.m.zhuravel@lpnu.ua

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318

METHOD OF COMPREHENSIVE ASSESSMENT OF THE EFFICIENCY OF APPLICATION OF CONTENT DISPOSAL AND RECONSTRUCTION TECHNOLOGY IN NETWORK INFRASTRUCTURE

The article explores the possibilities of using Content Disarm and Reconstruction (CDR) technology to increase the effectiveness of network resource protection during processing and transfer of files of various formats. The relevance of the study is due to the rapid increase in the dangers associated with the growth of the number of hidden threats implemented through legitimate file structures and capable of bypassing traditional means of detecting malicious content, which causes a high level of complexity in their prevention or neutralization. The main attention is focused on developing a method for comprehensive experimental assessment of the effectiveness of using CDR solutions as a means of preventive countermeasures against threats that arise during the exchange of files with potentially malicious content. The work considers the basics of the content security problem and the idea of its cleaning as one of the ways to solve it, as well as the principle of operation of the content disarm and reconstruction technology, which consists in removing active and potentially dangerous elements of the file with the subsequent formation of its safe copy based on the standard structure of the corresponding file format that was processed. The features of CDR application to various types of files, in particular documents, archives, images and multimedia content, are analyzed, and its advantages compared to classical signature and behavioral protection tools, such as antiviruses and sandbox detection methods, are also identified. An experimental methodology for mass testing CDR solutions on large volumes of files is proposed with further analysis of the results and formation of a system of quantitative performance indicators that take into account the level of neutralization of hidden threats, reconstruction correctness, processing performance and impact on network and computing resources. As a result, directions for further research are identified, in particular, clarification of optimal scenarios for the use of content neutralization and reconstruction technology, formalization of efficiency criteria and development of methods for optimizing performance while maintaining high quality of file reconstruction.

Keywords: cybersecurity; information protection; network security; content disarm.

Надійшла до редакції (Received): 17.05.2026
Прийнята до друку (Accepted): 12.06.2026
Опубліковано онлайн (Available online): 25.06.2026

УДК 004.85:004.414.2 DOI: 10.31673/2409-7292.2026.027419

Яценко Дмитро Володимирович
аспірант
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0009-0001-2610-222X
E-mail: d.yatsenko@stud.duikt.edu.ua

Садовенко Володимир Сергійович
кандидат фізико-математичних наук, доцент
Державний університет інформаційно-комунікаційних технологій, Київ, Україна
ORCID: 0000-0001-7341-6021
E-mail: v.sadovenko@duikt.edu.ua

ПАТЕРНИ ПРОЕКТУВАННЯ АРХІТЕКТУР ДЛЯ СИСТЕМ МАШИННОГО НАВЧАННЯ

У статті здійснено розширений систематизований огляд патернів проєктування архітектур для систем машинного навчання (ML-систем), що застосовуються під час розв’язання задач предиктивної аналітики в умовах динамічних бізнес-процесів і зростаючих обсягів даних. Обґрунтовано доцільність використання архітектурних патернів як формалізованих практик, що забезпечують структурованість, масштабованість, відтворюваність експериментів і керованість життєвим циклом моделей. Запропоновано багаторівневу класифікацію патернів за етапами життєвого циклу машинного навчання (збір, очищення та підготовка даних, інженерія ознак, навчання і валідація, розгортання, моніторинг, повторне навчання) та за архітектурними рівнями системи (рівень даних, рівень моделей, прикладний та інфраструктурний рівні). Проаналізовано функціональне призначення, переваги, потенційні ризики та обмеження застосування ключових патернів, зокрема Data Pipeline,

© Яцев А.В., Журавель І.М. Метод комплексного оцінювання ефективності застосування технології знешкодження та реконструкції контенту у мережевій інфраструктурі. Сучасний захист інформації, 2(66), 210–220. https://doi.org/10.31673/2409-7292.2026.029318