

ВІДГУК

офіційного опонента

професора кафедри систем та технологій кібербезпеки
Державного університету інформаційно-комунікаційних технологій

доктора технічних наук, професора

Казмірчук Світлани Володимирівни

на дисертаційну роботу Супруненка Іллі Олександровича

«Метод адаптивного логування комп'ютерних систем та програм»

подану на здобуття ступеня доктора філософії

за спеціальністю 123 Комп'ютерна інженерія

галузі знань 12 Інформаційні технології

Актуальність теми дисертаційного дослідження

Сучасні комп'ютерні системи функціонують у середовищі постійних змін: оновлюється програмний код, змінюється конфігурація, зростає кількість взаємодіючих компонентів і водночас скорочується допустимий час реагування на відмови та інциденти. За таких умов журнали подій є не лише засобом післяаварійного аналізу, а й одним із основних джерел даних для контролю стану системи та виявлення аномальної поведінки. Статично заданий рівень деталізації логування не завжди відповідає поточній ситуації: надмірна кількість записів створює інформаційний шум і додаткове навантаження, тоді як недостатня деталізація ускладнює встановлення причин збою або атаки. Тому дослідження способів зміни параметрів логування без зупинення прикладної системи має цілком визначену наукову і практичну потребу. Дисертаційна робота Супруненка І.О. спрямована на підвищення спостережності та оперативності контролю комп'ютерних систем і програм шляхом розроблення методу адаптивного логування. Обрана тема є актуальною, а поставлене науково-технічне завдання відповідає змісту спеціальності 123 – Комп'ютерна інженерія.

Зв'язок дисертації з науковими програмами, планами, темами

Результати дисертації пов'язані з науковими дослідженнями відповідно до Закону України «Про перспективні напрямки наукових досліджень» від 2006 року зі змінами від 2022 року. Отримані наукові результати включені в НДР Черкаського державного технологічного університету: «Інформаційна технологія психолінгвістичного аналізу тексту для стеганографічних систем» (ДР № 0123U102085), «Дослідження шляхів розвитку потокового шифрування на основі криптографічного кодування» (ДР № 0121U114389).

Обґрунтованість наукових положень, висновків та рекомендацій

Побудова дослідження є послідовною: від аналізу засобів забезпечення спостережності автор переходить до визначення вимог до адаптивного логування, формалізації функцій логування та реініціалізації, розширення моделей сигнатур динамічним варіантом повідомлення, а далі – до програмної реалізації й експериментальної перевірки. Для обґрунтування архітектурних рішень порівняно кілька механізмів міжпроцесової взаємодії; вибір сигналів Unix пов'язано з мінімальною кількістю додаткових залежностей та можливістю змінювати конфігурацію без перезапуску процесу. Висновки та

рекомендації дисертації логічно витікають зі змісту проведеного дослідження, відповідають поставленій меті та задачам, а рекомендації щодо практичного використання результатів є достатньо аргументованими з позиції спеціальності 123 – Комп’ютерна інженерія.

Достовірність одержаних наукових результатів

Достовірність результатів забезпечується коректним використанням методів аналізу та узагальнення, формалізацією сигнатур функцій, порівнянням альтернативних архітектурних рішень, програмною реалізацією запропонованого методу та проведенням обчислювального експерименту. Працездатність підходу перевірено на реалізації веб-сервера в середовищі Amazon Web Services із використанням EC2, Systems Manager Session Manager, Node.js і Docker. За наведеними в роботі даними, застосування адаптивного методу дало змогу підвищити інформативність лог-записів для досліджуваного компонента на 31%, уникнути втрати 14% клієнтських запитів під час реініціалізації та дещо краще відфільтрувати надлишкові повідомлення порівняно з базовим варіантом. Практичне використання результатів підтверджено відповідним актом впровадження.

Наукова новизна одержаних результатів

До основних положень наукової новизни належать:

- 1) вперше побудовані моделі сигнатур адаптивного логування шляхом формалізації та розширення сигнатур базової моделі, орієнтованої лише на критичність повідомлень, і введення функції реініціалізації, що дає змогу змінювати конфігурацію логування під час роботи системи;
- 2) вперше розроблений метод адаптивного логування, який поєднує моделі сигнатур із динамічним варіантом повідомлень та спрямований на підвищення спостережності та оперативності сигналювання про непередбачувані та критичні ситуації;
- 3) набули подальшого розвитку методи контролю роботи програм у хмарних середовищах завдяки впровадженню адаптивного логування з використанням хмарних сервісів.

Рівень наукової новизни, представлений у роботі є достатнім для дисертації рівня доктора філософії за спеціальністю 123 – Комп’ютерна інженерія.

Значення результатів роботи для практики

Практичне значення роботи полягає у доведенні запропонованого підходу до рівня алгоритмів, функціональних схем, методики застосування та ескізного програмного зразка. Реалізована можливість змінювати рівень критичності й перелік тегів без перезапуску процесу дає змогу оперативно збільшувати деталізацію для потрібного компонента, не втрачаючи повідомлень про помилки з інших частин системи.

Прикладну архітектуру розгорнуто в Amazon Web Services. Для адміністративного доступу використано штатні механізми AWS Systems Manager та IAM, а контейнеризація забезпечує відтворюваність перенесення програмних компонентів між середовищами. Результати дисертації використано у ТОВ «МОРОЗ ТЕХ» під час контролю коректності розроблення

програмного забезпечення системи дистанційного керування наземним самохідним роботизованим комплексом.

Наведені результати підтверджують прикладну придатність запропонованого методу, водночас межі його узагальнення визначаються умовами проведеного експерименту.

Оцінка структури та змісту дисертації

Дисертаційна робота Супруненка І.О. складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і двох додатків. Повний обсяг роботи становить 128 сторінок, з яких 115 сторінок основного тексту. Структура відповідає логіці поставлених завдань.

У *першому розділі* виконано аналіз сучасного стану розвитку інформаційних систем та програмного забезпечення, досліджено рівень загроз інформаційній безпеці та акценти сучасних технологій кібербезпеки. Акцентується увага на необхідності вдосконалення програмних засобів забезпечення аспекту спостережності.

У *другому розділі* обґрунтовано необхідність адаптивності логування, визначено вимоги до архітектури методу, формалізовано функції логування та реініціалізації. Для організації програмної архітектури запропоновано використання патернів «Фасад» і «Одинак» (Singleton), а для ініціювання зміни конфігурації – міжпроцесових сигналів Unix.

У *третьому розділі* розроблено динамічний варіант повідомлення, уточнено сигнатури методу та запропоновано підсистему валідації тіл динамічних функцій на основі аналізу абстрактного синтаксичного дерева з використанням JSON Schema.

У *четвертому розділі* подано прикладну архітектуру методу в хмарному середовищі, описано його реалізацію на базі AWS, Node.js і Docker та наведено результати порівняльного експерименту. Показано можливість змінювати параметри логування без зупинення веб-сервера та втрати його поточного стану.

Висновки дисертації містять узагальнення основних наукових та практичних результатів дослідження, відображають повноту виконання поставлених задач.

Відповідність технічного та стильового оформлення встановленим вимогам

Дисертація має цілісну структуру, ілюстративний матеріал пов'язаний із текстом, а основні позначення та терміни розкрито. Дисертаційна робота відповідає вимогам наукового стилю та загальноприйнятим нормам української мови. Текст роботи зрозумілий, технічна та наукова термінологія використані коректно.

Дотримання принципів академічної доброчесності

За результатами аналізу тексту дисертації та наведених посилань підстав стверджувати про порушення автором принципів академічної доброчесності не виявлено. Запозичені положення й матеріали супроводжуються посиланнями на відповідні джерела; особистий внесок здобувача у працях, підготовлених у співавторстві, зазначено.

Повнота оприлюднення результатів роботи та ступінь апробації

Основні результати дисертації оприлюднено у дев'яти наукових працях: п'яти статтях у фахових виданнях України категорії «Б», одному розділі колективної монографії та матеріалах трьох міжнародних науково-практичних конференцій. Тематика публікацій охоплює моделі сигнатур, механізми передавання повідомлень, динамічний варіант повідомлення, його валідацію та хмарну архітектуру адаптивного логування. Це дає підстави вважати результати дослідження оприлюдненими з достатньою повнотою.

Зауваження та дискусійні положення

1. Експеримент у підрозділі 4.5 проведено для одного прикладного сценарію веб-сервера та фіксованої послідовності запитів. У роботі не наведено результатів повторних прогонів, оцінок розкиду показників, довірчих інтервалів, а також вимірювань додаткового навантаження на процесор, пам'ять і підсистему введення-виведення. Через це отримані значення 31%, 61,3% і 14% переконливо характеризують наведений приклад, але поки що не дають достатніх підстав для широкого узагальнення ефективності методу.

2. Базою порівняння обрано логування, що фільтрує повідомлення лише за рівнем критичності. Для повнішого обґрунтування переваг запропонованого рішення доцільно було б порівняти його також із поширеними засобами структурованого логування, які підтримують динамічну зміну рівнів, контекстні поля, фільтри та централізоване керування конфігурацією. Інакше частина зафіксованого ефекту може пояснюватися обмеженістю базового варіанта, а не винятково властивостями авторського методу.

3. Динамічне формування та виконання коду істотно розширює поверхню атаки. Запропонована перевірка абстрактного синтаксичного дерева за JSON-схемою дає змогу контролювати структуру подання, проте сама по собі не гарантує безпечної поведінки функції під час виконання. У дисертації варто було чіткіше визначити модель загроз і довіри, а також розглянути ізоляцію виконання, обмеження доступних API та ресурсів, контроль цілісності конфігурації, журналювання адміністративних змін і механізм безпечного відкату.

4. Заявлена універсальність підходу щодо платформ, мов програмування та середовищ виконання підтверджена реалізацією на Node.js у Linux-сумісному середовищі AWS із використанням міжпроцесових сигналів. Питання перенесення методу на Windows, багатопроцесні та розподілені системи, оркестровані контейнери і короткоживучі serverless-функції залишилися поза експериментальною перевіркою. Тому межі застосовності методу слід було сформулювати точніше.

5. У роботі використовуються поняття «інформативність», «точність логування», «рівень спостережності» та «оперативність контролю», однак їх співвідношення і спосіб кількісного оцінювання визначено не в усіх випадках однозначно. Доцільно було б навести єдину систему показників із формальними визначеннями, одиницями вимірювання та умовами

інтерпретації. Це посилює б відтворюваність експерименту і зв'язок між заявленою науковою новизною та одержаними числовими результатами.

6. У тексті наявні окремі редакційні недоліки, зокрема «розробленого», «відлагодження», «що даду», «при логування», а також перевантажені речення і неусталене написання деяких англomовних термінів. Роботу доцільно додатково вчитати та уніфікувати термінологію відповідно до норм української науково-технічної мови.

Висловлені зауваження не заперечують наукової новизни та практичної цінності одержаних результатів і не впливають на загальну позитивну оцінку дисертаційної роботи. Водночас вони окреслюють питання, які доцільно врахувати під час подальшого розвитку методу та розширення сфери його застосування.

Висновок щодо відповідності дисертації встановленим вимогам

Дисертаційна робота Супруненка І.О. є завершеним самостійним науковим дослідженням, у якому розв'язано актуальне науково-технічне завдання підвищення рівня спостережності та оперативності контролю роботи комп'ютерних систем і програм шляхом розроблення та впровадження методу адаптивного логування. Одержані результати мають наукову новизну, практичне значення та достатній рівень апробації.

Вважаю, що дисертаційна робота Супруненка Іллі Олександровича «Метод адаптивного логування комп'ютерних систем та програм» за змістом, рівнем наукової новизни, обґрунтованістю положень і практичною цінністю дисертаційна робота відповідає вимогам Порядку присудження ступеня доктора філософії, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а її автор заслуговує на присудження ступеня доктора філософії за спеціальністю 123 – Комп'ютерна інженерія.

Опонент:

професор кафедри систем та технологій кібербезпеки
Державного університету
інформаційно-комунікаційних технологій,
доктор технічних наук, професор

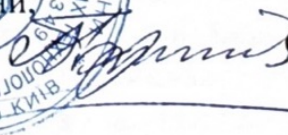


Світлана КАЗМІРЧУК

Підпис Казмірчук С.В. засвідчую:

Перший проректор
університету
комунікаційних технологій,
член-кореспондент НАН України,
доктор технічних наук, професор



 Олександр КОРЧЕНКО