

ВІДГУК

офіційного опонента на дисертаційну роботу

Драгунцова Романа Ігоровича

на тему «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності»,
представлену на здобуття ступеня доктора філософії
в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Актуальність теми дисертації.

Проблема достовірного оцінювання стану інформаційної системи завжди була однією з основних у теорії та практиці захисту інформації. Будь-яка процедура виявлення порушення спирається на певну множину вхідних відомостей. Якщо частина цих відомостей відсутня або суперечлива, змінюються умови, за яких здійснюється прийняття рішення щодо реагування. У дисертації ця загальна проблема розглядається стосовно комп'ютерних систем управління подіями безпеки за деградації інфраструктури.

За умов повномасштабної війни втрата електроживлення, каналів зв'язку та окремих компонентів інформаційно-комунікаційної системи не є одиничною відмовою. Вона впливає на доступність джерел подій, повноту телеметрії та узгодженість інвентарних даних. Внаслідок цього зростає ризик неправильної інтерпретації подій безпеки. Саме цей ризик і становить одну з центральних проблем дослідження.

Актуальність роботи визначається не лише обставинами воєнного часу. Питання оцінювання спостережності інформації та врахування неповноти телеметрії має значення для будь-яких розподілених інформаційно-комунікаційних систем, у яких стан об'єктів визначається за даними кількох джерел.

Оцінка обґрунтованості наукових результатів дисертації, їх достовірності та новизни.

Наукові результати одержано на основі функціонального і порівняльного аналізу, формалізації, математичного та комп'ютерного моделювання, синтезу архітектури й експериментальної перевірки. Для оцінювання роботи принциповим є те, що автор визначає перелік факторів ризику та сукупність параметрів, за якими стан втрати спостережності може бути виявлений і врахований під час обробки сигналів.

Наукова новизна здобутих результатів полягає в такому:

1. Розроблено постановку задачі підвищення спостережності інформації у контексті деградації інфраструктури, у якій поняття втрати спостережності визначається як стан системи, за якого зменшується повнота та/або достовірність телеметрії до рівня, що порушує коректність виконання щонайменше одного класу процедур інформаційної безпеки (виявлення, розслідування, атрибуція, реагування).

2. Дістав подальшого розвитку метод атрибутивного профілювання активів завдяки запропонованому вектору атрибутів, релевантних для

оцінювання спостережності та ризиків інтерпретації телеметрії за умов деградації інфраструктури.

3. Вперше запропоновано багатоконтурну архітектуру спостережності, в якій виділено контури інвентаризації та злиття даних про активи, аналітики подій/інцидентів, активного реагування, атрибутивного профілювання та обчислення правил/метрик, а також візуалізації та звітності, що дозволило розробити прототип відповідного технічного рішення.

4. Розроблено методологію, орієнтовану на корекцію процесів обробки сигналів в операційних центрах кіберзахисту, спрямовану на виявлення та врахування деградації спостережності як необхідної умови коректної інтерпретації сигналів про кіберзагрози за умов воєнних впливів.

З позиції теорії інформаційної безпеки суттєвим є подальший розвиток атрибутивного профілювання активів. У запропонованому векторі атрибутів враховано параметри, які характеризують умови достовірної інтерпретації телеметрії, що відповідає задачам аналізу та оцінювання ризиків.

Експериментальна перевірка підтверджує, що врахування деградації спостережності змінює результати обробки подій у передбаченому напрямі та дає змогу відокремлювати технічну деградацію від сигналів про кіберзагрози. Достовірність цих висновків слід відносити до умов проведеного експерименту; поширення на інші класи інфраструктури потребує додаткових випробувань.

Оцінка змісту дисертації, її завершеність та дотримання принципів академічної доброчесності.

Дисертація побудована як завершене дослідження однієї науково-прикладної задачі. Структурні частини роботи не є самостійними оглядами різних аспектів кібербезпеки, а підпорядковані послідовному виконанню завдань, визначених у вступі. Аналіз існуючих методів і факторів впливу формує вихідні умови; формалізована модель визначає зв'язок деградації інфраструктури зі станом спостережності; розроблені методи задають порядок врахування цього стану; архітектура і прототип забезпечують технічну реалізацію; експеримент перевіряє одержані положення.

За такої структури наукова новизна зосереджена в постановці задачі, розвитку методу атрибутивного профілювання, багатоконтурній архітектурі спостережності та методології корекції процесів обробки сигналів. Прикладні засоби, використані у прототипі, виконують функцію реалізації та перевірки цих положень.

За поданим текстом дисертації, системою бібліографічних посилань та відомостями про особистий внесок здобувача підстав для висновку про некоректне використання результатів інших авторів не встановлено. Результати спільних публікацій супроводжуються визначенням особистого внеску здобувача. У вступі окремо зазначено використання інструменту штучного інтелекту для орфографічного, стилістичного та редакційного опрацювання тексту з покладенням відповідальності за прийняті правки на автора. Формальна оцінка текстових збігів має здійснюватися відповідно до процедури академічної доброчесності установи.

Мова та стиль викладення результатів.

Робота написана українською мовою. Виклад відповідає науковому та офіційно-діловому стилю, прийнятому для кваліфікаційних наукових праць. У тексті доцільно зберігати саме той понятійний апарат, який визначено у вступі: «спостережність інформації», «втрата спостережності», «телеметрія», «інвентарні дані», «деградація інфраструктури», «атрибутивне профілювання активів», «ризики інтерпретації телеметрії».

Окремі терміни в основному тексті використовуються з варіаціями. Для остаточної редакції бажано усунути такі відмінності та виправити технічні помилки нумерації. Поняття, що мають усталене значення в теорії захисту інформації та комп'ютерних наук, не потребують введення додаткових авторських синонімів.

Оприлюднення результатів дисертаційної роботи.

Основні положення дисертаційної роботи висвітлено у наукових публікаціях здобувача, безпосередньо пов'язаних із тематикою дослідження. Публікації охоплюють питання впливу деградації інфраструктури на кібербезпеку, спостережності інформації, динамічних компонентів інформаційно-комунікаційних систем, моніторингу під час відключень електропостачання та функціонування операційних центрів кіберзахисту в умовах повномасштабної війни.

Послідовність оприлюднення результатів відповідає розвитку дисертаційного дослідження: від постановки проблеми та аналізу факторів впливу до формалізації окремих характеристик, розроблення методів і їх експериментальної перевірки. Зміст опублікованих праць відповідає положенням, винесеним на захист.

Оприлюднення результатів охоплює як постановку проблеми, так і окремі складові запропонованого підходу. Це дає підстави вважати, що основні наукові положення дисертації пройшли належну апробацію.

Недоліки та зауваження до дисертаційної роботи.

1. Автор добре проаналізував недоліки відомих підходів, але критерії, за якими наприкінці доводить перевагу власних розробок не визначив.

2. Некоректна структура окремих положень наукової новизни. Так, у пунктах 1,2,4 новизни не зазначений досягнутий ефект, а у п. 4 – не визначено ступінь новизни та за рахунок чого досягається ефект.

3. У практичній цінності не визначено в яких організаціях може використовуватися або використовуються результати досліджень, що підкріплюється актами впровадження.

4. Ризик інтерпретації телеметрії в роботі використовується як прикладна характеристика для пріоритезації та вибору дій. Його слід чітко відмежовувати від загального ризику інформаційної безпеки, який охоплює ймовірність реалізації загрози та наслідки для об'єкта.

5. Формалізована модель має дескриптивний характер. Для одержання прогнозних оцінок необхідне визначення параметрів моделі на репрезентативних даних та перевірка їх стійкості для різних інформаційно-комунікаційних систем.

6. Експериментальна перевірка виконана у контрольованих умовах. Для оцінювання статистичної стійкості результатів доцільні повторні серії випробувань із варіюванням інтенсивності втрати телеметрії, часу відновлення та складу активів.

Висловлені зауваження стосуються переважно меж оцінювання та подальшого розвитку параметричного апарату. Вони не ставлять під сумнів основні результати та позитивну оцінку дисертації.

Висновок про дисертаційну роботу.

Дисертаційна робота Драгунцова Романа Ігоровича «Методи збору, обробки та аналізу інформації в комп'ютерних системах управління подіями безпеки в умовах обмеженої спостережності» є завершеною кваліфікаційною науковою працею. У ній розв'язано актуальну науково-прикладну задачу підвищення ефективності процесів збору та аналізу інформації за деградації інфраструктури інформаційно-комунікаційних систем.

Наукові результати мають належне обґрунтування, містять визначені положення новизни та доведені до експериментальної перевірки. Робота відповідає предметній області спеціальності 122 Комп'ютерні науки.

Вважаю, що дисертаційна робота за актуальністю, науковою новизною, обґрунтованістю результатів і практичним значенням відповідає вимогам чинного законодавства України, передбаченим пунктами 6–9 Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради, затвердженого постановою Кабінету Міністрів України від 12 січня 2022 р. № 44, а Драгунцов Роман Ігорович заслуговує на присудження ступеня доктора філософії в галузі знань 12 Інформаційні технології за спеціальністю 122 Комп'ютерні науки.

Офіційний опонент:

Перший проректор Державного університету
інформаційно-комунікаційних технологій,
член-кореспондент НАН України,
доктор технічних наук, професор,
лауреат Державної премії України
в галузі науки і техніки,
Заслужений діяч
науки і техніки України

Олександр КОРЧЕНКО