Голові спеціалізованої вченої ради Д 26.185.01
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
член-кореспонденту НАН України, доктору
технічних наук, професору Мохору В.В.
03164, м. Київ, вул. Генерала Наумова, 15

ВІДГУК
офіційного опонента

професора кафедри обчислювальної техніки та програмування Національного технічного університету «Харківський політехнічний інститут», доктора технічних наук, доцента Гавриленко Світлани Юріївни на дисертаційну роботу Комарова Максима Юрійовича «Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти

Актуальність теми досліджень

Активне впровадження комп'ютерних систем в усі види діяльності суспільства, постійне зростання їх обчислювальної потужності, використання комп'ютерних мереж різного масштабу суттєво розширило можливості зловмисників у використанні методів і засобів несанкціонованого доступу до інформації, об'єктивно збільшило кількість зовнішніх чинників та особливостей їх впливу на повсякденну експлуатацію сучасних комп'ютерних систем. Експлуатація таких складних технічних систем на сучасному етапі усе більшою мірою стикається з проблемами забезпечення інформаційної та функціональної безпеки.

У той же час рівень розвитку засобів діагностування й ідентифікації деструктивних змін режимів функціонування і внутрішніх характеристик комп'ютерних систем та мереж на сьогодні не можуть гарантувати необхідний рівень захисту інформації.

Найбільш актуальним це питання стоїть в комп'ютерних системах та мережах об'єктів критичної інфраструктури, в яких нехтування питаннями

безпеки даних може завдати значної шкоди як суспільству взагалі, так і кожній окремій людині зокрема.

Тому вирішення науково-технічної проблеми, що виникає на підґрунті наукового протиріччя між збільшенням рівня загроз безпеки даних і розширенням різноманіття зовнішніх деструктивних впливів, з одночасним невідповідним рівнем методів та засобів ідентифікації цих загроз, полягає в розробці нових та удосконаленні існуючих методів і засобів для захисту інформації в комп'ютерних системах та мережах об'єктів критичної інфраструктури в умовах зовнішніх впливів, є актуальним та таким, що має важливе науково-прикладне і практичне значення.

Відповідно до зазначеного, дисертаційна робота Комарова М.Ю. є актуальною, спрямована саме на підвищення рівня захисту інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури, шляхом розробки відповідного методу та засобів захисту інформації. Крім того, тема дисертаційних досліджень безпосередньо пов'язана з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014–2018 роки», «Планом проведення ДержНДІ Спецзв'язку науково-дослідних та дослідно-конструкторських робіт за основними напрямами науково-технічної діяльності Держспецзв'язку в 2018 році (Зведений тематичний план. Частина 2)» №01/02/02-96т від 02.03.2018, «Планом проведення ДержНДІ Спецзв'язку науково-дослідних та дослідно-конструкторських робіт за основними напрямами науково-технічної діяльності Держспецзв'язку в 2019 році (Зведений тематичний план. Частина 2)» №01/02/02-117т від 27.03.2019, Стратегією національної безпеки України від 26.05.2015 № 287/2015, Стратегією кібербезпеки України від 15.03.2016 № 96/2016.

Загальна характеристика дисертаційної роботи

В цілому дисертаційна робота є завершеним науковим дослідженням, яке включає анотацію, вступ, чотири розділи, висновки, 2 додатки, список використаних джерел, що налічує 102 найменування.

У анотації та вступі представлена загальна характеристика дисертації, обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету і задачі дослідження, визначено наукову новизну отриманих результатів та їх практичне значення, наведено інформацію про впровадження результатів, їх апробацію та публікації, структуру, об'єм та ключові слова.

У першому розділі проведено аналіз основних нормативно-правових документів, які регламентують питання забезпечення кібербезпеки інформаційних систем об'єктів критичної інфраструктури в України.

Виконано аналіз існуючих робіт та підходів щодо таксономії загроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інфраструктури. Описано основні підходи до створення таксономій кіберзагроз.

У заключній частині розділу сформульовано мету та здійснено постановку наукового завдання дисертаційного дослідження.

У другому розділі розроблено таксономію кіберзагроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури, складено матрицю залежності інформаційних об'єктів захисту від типу потенційних загроз, що можуть на них впливати, та схильності до конкретних загроз, а також розроблено модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних систем та мереж об'єктів критичної інформаційної інфраструктури.

У запропонованій Комаровим М.Ю. таксономії розроблено комбінований підхід до вирішення задачі класифікації, де на відміну від попередніх робіт, вводиться ієрархічна структура відносин з деревовидним розкриттям категорій. Як самостійний окремий об'єкт вводиться важливе поняття «етап атаки», що дозволяє, на відміну від попередніх підходів,

досить природним чином описувати багатоетапні атаки, які є досить розповсюдженими на сьогоднішній день.

У третьому розділі розроблено метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних систем та мереж об'єктів критичної інфраструктури, який ґрунтується на способі моніторингу трафіку, що надходить до відомчої інформаційно-телекомунікаційної системи з глобальної мережі Інтернет та призначений для застосування у багаторівневій системі виявлення підозрілих впливів, яка здійснює моніторинг, аналіз та обробку покажчиків вхідного трафіку.

Запропоновано структурну модель багаторівневої системи виявлення підозрілих впливів на комп'ютерні системи та мережі об'єктів критичної інфраструктури. Розроблено методику оцінювання кіберстійкості комп'ютерних систем та мереж об'єктів критичної інфраструктури.

У четвертому розділі розроблено алгоритм функціонування багаторівневої системи виявлення підозрілих впливів та програмний застосунок, який реалізує даний алгоритм, проведено експериментальні дослідження систем захисту інформації комп'ютерних систем та мереж об'єктів критичної інфраструктури. На основі запропонованого методу та розроблених засобів створено комплексну систему захисту інформації захищеного вузла Інтернет доступу «Фарлеп-Інвест» та здійснено державну експертизу комплексної системи захисту інформації в автоматизованій інформаційній системі «Централізована база даних перенесених номерів» державного підприємства «Український державний центр радіочастот». Отримані результати підтверджують функціонування системи захисту інформації комп'ютерних систем та мереж об'єктів критичної інфраструктури, створеної на основі розроблених у дисертації методу та засобів та їх успішне практичне застосування.

У висновках наведено основні отримані результати, їх наукову та практичну цінність, дані щодо впровадження результатів роботи.

У додатках наведено документи, що підтверджують впровадження результатів дисертації, та лістинги (коди) програмних засобів.

Наукова новизна результатів дисертації

Основні наукові результати дисертаційної роботи:

– вперше розроблено таксономію кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання ієрархічної структури відносин з деревовидним розкриттям категорій, дозволяє описувати багатоетапні атаки, які на сьогоднішній день отримали дуже широку розповсюдженість;

– вперше розроблено модель бази даних кіберзагроз інформаційним об'єктам захисту комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, яка за рахунок використання параметрів загроз, визначених та класифікованих з використанням розробленої таксономії кіберзагроз, їх характеристик, параметрів заходів протидії та параметрів властивостей інформації, що підлягає захисту, дозволяє розробити базу даних кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури;

– вперше розроблено комбінований метод розпізнавання кіберзагроз інформаційній безпеці комп'ютерних мереж та систем об'єктів критичної інформаційної інфраструктури, який за рахунок поєднання сигнатурного методу та методу виявлення аномалій, дозволяє розширити спектр виявлених кіберзагроз.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, та їх достовірність

Обґрунтованість та достовірність наукових положень, висновків і рекомендацій дисертації забезпечується коректним використанням відповідного математичного апарату і підтверджується співставленням з результатами експериментальних досліджень.

Практична значимість

Основні практичні результати дисертаційної роботи полягають у тому, що:

– розроблено алгоритмічне забезпечення на основі запропонованого комбінованого методу розпізнавання кіберзагроз для реалізації відповідного програмного засобу, що дозволяє здійснювати автоматизоване розпізнавання кіберзагроз та здійснювати захист від них;

– розроблено алгоритмічне забезпечення на основі запропонованої методики оцінювання кіберстійкості для реалізації відповідного програмного засобу, що дозволяє здійснювати автоматизований розрахунок кіберстійкості з урахуванням таких показників як кібернадійність, кіберзахищеність та кіберстійкість;

– на основі запропонованих алгоритмів розроблений програмний застосунок, що використовує запропоновану методику для захисту інформації в комп'ютерних мережах та системах об'єктів критичної інфраструктури.

Результати теоретичних та практичних досліджень знайшли застосування у таких науково-дослідних роботах:

– «Розробка методів оцінювання чутливості Об'єднаної енергосистеми України до кібернетичних впливів» (шифр «ВПЛИВ», державний реєстраційний номер 0118U005320);

– «Розроблення методів забезпечення кібербезпеки функціонування Об'єднаної енергетичної системи України в рамках впровадження концепції інтелектуальних мереж» (шифр «ІНТЕЛЕНЕРГО», державний реєстраційний номер 0119U101856).

Апробація результатів роботи та публікації

Результати дисертаційних досліджень, які виносяться на захист, опубліковані автором у 22 наукових працях, у тому числі: 9 наукових статей у фахових наукових журналах та збірниках наукових праць, з яких 5 – у наукових журналах, що індексуються міжнародними наукометричними базами даних, 1 патент України на корисну модель, 1 свідоцтво про реєстрацію авторського права на твір, а також 11 матеріалів та тез доповідей конференцій.

Перераховані публікації з достатньою повнотою відображають наукові та практичні результати дисертації та відповідають вимогам до публікацій результатів дисертації на здобуття наукового ступеня кандидата наук.

Відповідність автореферату дисертаційній роботі

Зміст автореферату повністю відображає зміст дисертаційної роботи та розкриває її суть. Дисертація і автореферат відповідають вимогам до їх оформлення.

Відповідність паспорту спеціальності

Основні наукові та практичні результати роботи пов'язані із захистом інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури, відповідають паспорту спеціальності 05.13.05 – комп'ютерні системи та компоненти, а саме напрямкам досліджень «Теоретичні основи, методи і апаратно-програмні засоби комп'ютерної криптографії, розподілу доступу та захисту інформації в комп'ютерних системах та мережах».

Зауваження до змісту дисертації:

1) У вступі нечітко обґрунтовано актуальність дисертаційної роботи, а саме: чому (стр. 12) незважаючи на значну кількість підходів до вирішення даної проблеми, вона залишається актуальною не тільки для України, але і для всієї світової спільноти.

2) У першому розділі майже відсутній аналіз сучасних методів та засобів захисту інформації в комп'ютерних мережах та системах, не наведено обмеження їх використання.

3) У третьому розділі вперше розроблено комбінований метод розпізнавання кіберзагроз інформаційній безпеці, який поєднує сигнатурний метод та метод виявлення аномалій, але в роботі відсутня будь-яка інформація які саме типи аномалій і яким чином він розпізнає.

4) На стр. 92 наведено методику оцінки кіберстійкості об'єкту, де одною із складових методики є оцінка коефіцієнта пов'язаності елемента і його внесок в цільову функцію об'єкта. Нажаль, раніше не наведено визначення коефіцієнта пов'язаності і яким чином він розраховується.

5) В формулі (10) визначено критерій здатності об'єкта КІ виконувати цільову функцію в умовах деструктивного інформаційного впливу. Надалі, по тексту не зрозуміло яким чином визначаються показники H_1-H_4, які визначають значення цього критерію.

6) Четвертий розділ містить надлишкову інформацію щодо призначення загальної структури та алгоритмів функціонування централізованої бази даних перенесених номерів» ДП «Український державний центр радіочастот», на базі якої проводились експериментальні дослідження з метою підтвердження теоретичних положень та практичних розробок дисертаційного дослідження.

7) В роботі не виконано порівняльний аналіз теоретичних положень та практичних розробок дисертаційного дослідження з відомими методами з метою оцінки їх ефективності (стр.137).

Дані недоліки не ставлять під сумнів основні наукові та практичні результати дисертаційної роботи і суттєво не впливають на її загальну позитивну оцінку.

Висновок

У дисертаційній роботі «Метод та засоби захисту інформації від кібервпливів в комп'ютерних системах та мережах об'єктів критичної інфраструктури» Комарова Максима Юрійовича вирішено актуальну науково-прикладну задачу, пов'язану з підвищенням рівня захисту інформації від кібервпливів в комп'ютерних мережах та системах об'єктів критичної інформаційної інфраструктури. Дисертація є завершеною науково-дослідною роботою. За актуальністю вибраної теми, достовірністю і обгрунтованістю висновків, новизною досліджень, значенням отриманих

результатів для науки і практики дисертаційна робота відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 № 567, а її автор – Комаров Максим Юрійович заслуговує присудження йому наукового ступеня кандидата технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти.

Офіційний опонент
професор кафедри
обчислювальної техніки та програмування
Національного технічного університету
«Харківський політехнічний інститут»
МОН України,
доктор технічних наук, доцент
Гавриленко Світлана Юріївна

Підпис _____
ЗАСВІДЧУЮ:
ВЧЕНИЙ СЕКРЕТАР
НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
"ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"
_____ Заховоротний О.Ю.
"28" 09 2021 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний технічний університет "Харківський політехнічний інститут" * код 02071180 *