ВІДГУК

офіційного опонента про дисертаційну роботу Корченко Анни Олександрівни «Методи ідентифікації аномальних станів для систем виявлення вторгнень», подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації

1. **Актуальність теми дисертаційної роботи та її зв'язок з науковими програмами, планами, темами.**

В останні роки відбувається значне збільшення обсягів інформації, що накопичується, зберігається та оброблюється за допомогою інформаційних систем. При цьому концентрування в єдиних базах даних інформації різного призначення та різної належності і різке розширення кола користувачів, що мають безпосередній доступ до ресурсів інформаційної системи, породжують проблему забезпечення їх захисту від різного роду вторгнень. Зростання складності апаратно-програмних засобів та існуючі недоліки сучасних ІТ призводять до постійного збільшення методів зламу захисту і, як наслідок, до вторгнення в інформаційну систему з метою порушення її нормального функціонування. Для запобігання цьому створюються системи виявлення вторгнень (СВВ), які є невід'ємною частиною будь-якої сучасної системи безпеки, а світова тенденція свідчить про те, що виявлення вторгнень, стане обов'язковою функцією операційної системи та вже застосовується в різному програмному забезпеченні. Тому вибір об'єкту дисертаційного дослідження – процесу виявлення аномальних станів, утворених атакуючими діями на ресурси інформаційних систем є актуальним та доцільним.

Варто відзначити, що існує певна проблема ефективного використання систем виявлення вторгнень, яка обумовлена протиріччям між необхідністю моніторингу та блокування нових видів кібератак за максимально короткий час і високою інерційністю існуючих СВВ щодо їх адаптації до виявлення аномалій, породжених реалізацією нових типів загроз ресурсам інформаційної системи. Тому виникає потреба розширення функціональних можливостей таких систем за рахунок впровадження функцій виявлення раніше невідомих кібератак (зокрема, 0-day атак), що характеризуються невстановленими або нечітко визначеними критеріями. Тому вибір предмету дисертаційного дослідження – моделі, методи, засоби та системи виявлення аномалій, утворених атакуючими діями на ресурси інформаційних систем, та визначення мети дослідження – розширення функціональних можливостей сучасних систем виявлення вторгнень, шляхом розробки методології побудови систем виявлення за максимально короткий час аномальних станів, породжених новими видами кібератак, є обґрунтованими та відповідають темі дисертаційної роботи.

Тема досліджень та одержані результати безпосередньо пов'язані з «Основними науковими напрямами та найважливішими проблемами фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук НАН України на 2014-2018 роки», «Стратегією національної безпеки України» від 26 травня 2015 року № 287/2015, «Стратегією кібербезпеки України» від 15 березня 2016 року №96/2016 та науково-дослідними роботами «Методи та моделі виявлення уразливостей в ресурсах інформаційних систем» (2015-2017 рр.) № 25/09.01.08, «Системи мультирівневого розмежування доступу до інформаційних ресурсів», (2018-2019 рр.) № 19/14.01.05 від 01.09.2018 р., в яких здобувач був науковим керівником та відповідальним виконавцем.

Таким чином, усе сказане обумовлює актуальність теми дисертаційної роботи Корченко А.О. і наукову новизну поставлених в ній задач досліджень.

2. Наукова новизна результатів роботи

У результаті виконання дисертаційної роботи набув подальшого розвитку науковий напрям, пов'язаний із розробленням методології створення систем виявлення вторгнень.

Виходячи з того, що нові наукові результати - це нові знання в певній галузі фундаментальних чи прикладних наук, можна вважати основними науковими результатами дисертації таке:

- вперше розроблену кортежну модель формування атакуючих середовищ, яка за рахунок формалізації процесу створення m_i-вимірних параметричних, атакуючих, еталонних, поточних та детекційних підсередовищ, дозволяє сформувати набір часткових кортежів, за якими здійснюється симуляція процесу виявлення аномального стану в m-вимірному гетерогенному параметричному середовищі, утвореного відповідним атакуючим середовищем у заданий часовий проміжок;

- вперше розроблений метод формування еталонного середовища, який за рахунок використання множини ідентифікаторів лінгвістичних оцінок та ідентифікаторів інтервалів, базової та похідної матриці частот, формального відображення суджень експерта для характеристики поточного стану параметрів відносно кібератаки, процесу формування на заданих інтервалах частот зустрічальності експертних оцінок та підмножин нечітких термів, дозволяє формалізувати процес отримання еталонних значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризує конкретне еталонне підсередовище;

- вперше розроблені методи фазифікації та дефазифікації параметрів, які на основі еталонних підсередовищ, поправкових і лінгвістичних еталонів підмножин інтервалів для формування частот зустрічальності значень фізичних параметрів у задані моменти очікуваної події та процедури визначення допоміж-

ного терма, експертних коефіцієнтів параметрів і кібератаки, що характеризують експертні лінгвістичні оцінки, пов'язані з рівнем аномального стану в поточному середовищі дозволяють формалізувати процес перетворення значень параметрів m-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану та відобразити параметри детекційного середовища, що характеризують у числовій формі рівень упевненості експерта відносно його суджень щодо можливих кібератак;

- вперше розроблений метод α-рівневої номіналізації нечітких чисел, який за рахунок побудованого механізму формування множини α-рівней, допоміжних підмножин α-рівневих інтервалів та міжточкових α–рівневих інтервалів, а також процесу номіналізації та визначення значень необхідних супортів нечітких чисел еталонних та поточних середовищ, дозволяє здійснити графічну інтерпретацію нечітких величин та визначати ідентифікуючі терми, що відображають поточні стани еталонних та поточних підсередовищ, які характерні для реалізації певних типів кібератак на ресурси інформаційних систем;

- вперше розроблений метод визначення ідентифікуючих термів, який за рахунок базового механізму, що реалізує формування елементів множини характерних ознак та використання узгодженої функції, дозволяє за допомогою еталонного середовища здійснити пошук ідентифікуючих перетворених еталонних термів, орієнтованих на обробку в детекційному середовищі для визначення рівнів аномальних станів;

- вперше розроблений метод формування детекційного середовища, який на основі запропонованої кортежної моделі за рахунок механізму формування підмножин ідентифікаторів аномальності, формалізації процесу побудови вирішальних функцій та умовних детекційних виразів, дозволяє сформувати необхідну множину детекційних правил, що використовуються для визначення рівней аномальних станів, характерних впливу певних типів кібератак;

- вперше розроблену методологію побудови систем виявлення аномалій породжених кібератаками, яка за рахунок механізмів формування атакуючих середовищ, побудови m-вимірних параметричних еталонних та поточних підсередовищ, α-рівневої номіналізації еталонних та поточних підсередовищ, процесу дефазифікації та визначення ідентифікуючих термів та формування детекційних середовищ дозволяє будувати системи, що використовуються для визначення рівня аномального стану в m-вимірному гетерогенному параметричному середовищі;

- вперше розроблене структурне рішення обчислювальної системи виявлення кібератак, яке за рахунок баз даних кібератак, правил та еталонів, а також модулів формування поточних значень, α-рівневої номіналізації, дефазифікації та ідентифікуючих термів, рівня аномальності та візуалізації дозволяє будувати

засоби, які визначають рівні аномального стану, що характерні впливу певного типу кібератак і розширюють функціональні можливості сучасних систем виявлення вторгнень.

3. **Ступінь обґрунтованості наукових положень дисертації та їх достовірність.**

Наукові положення, викладені в дисертаційній роботі, є достатньо обґрунтованими за рахунок використання апробованих математичних методів та елементів теорій, а саме: методів системного аналізу, прийняття рішень, моделювання, експертного оцінювання; елементів теорії множин, теорії нечітких множин, теорії алгоритмів; елементів нечіткої логіки.

Достовірність основних наукових результатів роботи підтверджується наведеною в розд. 2-5 системою формальних методик і перетворень, що не містить принципових помилок, а також рядом прикладів і збіжністю результатів експериментальних досліджень, отриманих під час програмної реалізації алгоритмів виявлення аномальних станів.

4. Цінність дисертаційної роботи для науки

Цінність дисертації полягає в тому, що в ній запропоновано нове рішення важливої науково-технічної проблеми в теорії побудови та використання систем виявлення вторгнень. Змістовний аспект запропонованого рішення, який спрямований на розширення класу моделей і методів ідентифікації аномальних станів, що забезпечують розширення функціональних можливостей сучасних систем виявлення вторгнень, не був відомий раніше.

5. **Практична корисність роботи**

Практична корисність роботи обумовлена тім, що використання запропонованих в ній моделей, формальних методів, конкретних рішень і рекомендацій дозволяє створювати більш досконалі, порівняно з відомими, програмні засоби виявлення аномальних станів, які можуть застосовуватися автономно або як розширювачі функціональних можливостей сучасних систем виявлення вторгнень.

Результати дисертаційних досліджень впроваджено в ТОВ «Сайфер БІС», а також використовуються в навчальному процесі кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, кафедри інформаційної безпеки Інституту інформаційних та телекомунікаційних технологій Казахського національного дослідного технічного університету ім. К.І. Сатпаєва і кафедри інформатики та автоматики Технічно-гуманістичної академії у Бельско-Бялій (Польща).

6. **Оцінка змісту дисертації, її завершеності й оформлення.**

Побудова дисертації відповідає прийнятим для наукового дослідження вимогам. Дисертація складається з анотації, списку скорочень, вступу, п'яти розділів, загальних висновків, додатків, списку використаних джерел до кожного розділу

У вступі обґрунтовано актуальність теми дисертаційної роботи, показано зв'язок роботи з науковими темами, сформульовано мету та задачі досліджень, наведено методи дослідження, викладено наукову новизну та практичне значення одержаних результатів, зазначено особистий внесок здобувача та наведено відомості про впровадження, апробації, структуру роботи.

У першому розділі проведено дослідження науково-технічної проблеми, пов'язаної з розробкою методів ідентифікації аномальних станів для систем виявлення вторгнень (СВВ) та в результаті аналізу сучасних СВВ та їх компонентів визначені вимоги до СВВ, які можуть бути побудовані на основі підходу, що використовує математичний апарат нечітких множин.

Другий розділ присвячений розробці кортежної моделі та методів формування етлонних середовищ для ідентифікації аномальних станів. В основу розробленої кортежної моделі формування атакуючих середовищ (КМАС) покладено m-вимірні параметричні, атакуючі, еталонні, поточні та детекційні підсередовища, на основі яких сформовано набір часткових кортежів. За допомогою сформованого кортежу визначається стан аномальності в m-вимірному гетерогенному параметричному середовищі, яке утворюється не тільки атакуючим середовищем в певний момент часу, але і середовищами з іншими классами кібератак, для яких можна сформувати подібні кортежі.

На основі КМАС розроблено метод формування еталонних середовищ (МФЕС), який за рахунок використання множини ідентифікаторів лінгвістичних оцінок та ідентифікаторів інтервалів, базової та похідної матриці частот, формального відображення суджень експерта для характеристики поточного стану параметрів відносно кібератаки, процесу формування (на заданих інтервалах) частот зустрічальності експертних оцінок та підмножин нечітких термів, забезпечує можливість формалізувати процес отримання еталонних значень фіксованих параметрів заданих груп лінгвістичних змінних, що характеризує конкретне еталонне підсередовище.

Також, базуючись на МФЕС, розроблено метод формування еталонного підсередовища для виявлення сніфінг-атак та метод побудови еталонів лінгвістичних змінних для систем виявлення email-спуфінг-атак.

Третій розділ присвячений розробці набору базових методів формування поточного середовища, що складається з методів фазифікації параметрів, номіналізації нечітких чисел (НЧ), визначення ідентифікуючих термів.

Метод фазифікації параметрів на еталонних підсередовищах (МФП) за рахунок введених множин сенсорів, лічильників та поправкових еталонів, а також використання множин лінгвістичних еталонів та відповідних підмножин інтервалів для формування частот зустрічальності значень фізичних параметрів у задані моменти очікуваної події, дозволяє формалізувати процес перетворення поточних значень параметрів m-вимірних поточних середовищ для їх подальшого застосування у виявленні аномального стану.

Метод α-рівневої номіналізації НЧ (МАН) за рахунок побудованого механізму формування множини α-рівней, допоміжних підмножин α-рівневих та міжточкових α-рівневих інтервалів, а також процесу номіналізації та визначення значень необхідних супортів НЧ еталонних та поточних середовищ, дозволяє здійснити графічну інтерпретацію нечітких величин та визначати ідентифікуючі терми, що відображають поточні стани еталонних та поточних підсередовищ.

Метод визначення ідентифікуючих термів (МВІТ) за рахунок базового механізму, що реалізує формування елементів множини характерних ознак та використання узгодженої функції, дозволяє за допомогою еталонного середовища здійснити пошук ідентифікуючих перетворених еталонних термів, орієнтованих на обробку в детекційному середовищі для визначення рівнів аномальних станів.

Запропоновані методи МФП, МАН і МВІТ забезпечують можливість формалізувати процес перетворення в нечітку форму поточних значень параметрів m-вимірних поточних середовищ, визначати ідентифікуючі терми, що відображають стан еталонних і поточних підсередовищ, та за допомогою еталонного середовища здійснити пошук ідентифікуючих перетворених еталонних термів для визначення рівней аномальних станів.

Четвертий розділ присвячений розробці методів дефазифікації параметрів і формування детекційного середовища та методології побудови систем виявлення аномалій.

Метод дефазифікації параметрів детекційного середовища за рахунок процедури визначення допоміжного терма, експертних коефіцієнтів (ЕК) параметрів та ЕК кібератаки, що характеризують експертні лінгвістичні оцінки, пов'язані з рівнем аномального стану в поточному середовищі, дозволяє у числовій формі відобразити рівень упевненості експерта відносно його суджень щодо можливих кібератак.

Метод формування детекційного середовища (МФДС), який базується на запропонованій кортежній моделі, за рахунок механізму формування підмножин ідентифікаторів аномальності, формалізації процесу побудови вирішальних функцій та умовних детекційних виразів, дозволяє сформувати необхідну

множину детекційних правил, що використовуються для визначення рівней аномальних станів, характерних впливу певних типів кібератак.

На основі КМАС та методів МФЕС, МФП, МАН, МВІТ, МДП і МФДС розроблена методологія побудови систем виявлення аномалій (МПСВ), породжених кібератаками, яка за рахунок механізмів формування атакуючих середовищ, побудови m-вимірних параметричних еталонних та поточних підсередовищ, α-рівневої номіналізації еталонних та поточних підсередовищ, процесу дефазифікації та визначення ідентифікуючих термів і формування детекційних середовищ дозволяє будувати системи, що використовуються для визначення рівня аномального стану в m-вимірному гетерогенному параметричному середовищі.

П'ятий розділ присвячений розробці засобів розширення функціональних можливостей СВВ. На основі запропонованої методології розроблено структуру обчислювальної системи виявлення кібератак (СВК), яка за рахунок баз даних кібератак, правил та еталонів, а також модулів формування поточних значень, α-рівневої номіналізації, дефазифікації та ідентифікуючих термів, рівня аномальності та візуалізації дозволяє будувати засоби, які визначають рівні аномального стану, що характерні впливу певного типу кібератак і розширюють функціональні можливості сучасних СВВ.

На базі запропонованої методології та структурованого рішення обчислювальної системи розроблено алгоритмічне забезпечення для реалізації відповідного ПЗ виявлення кібератак.

Наведено результати експериментальних досліджень, які здійснювалися за допомогою розробленої віртуальної мережі, шляхом моделювання 2000 атак (з достатньо високим рівнем впливу на файл-сервер), кожна з яких була виявлена за допомогою певного умовного виразу сформованого детекційного середовища. Ці результати підтверджують достовірність основних теоретичних положень, практичних розробок та висновків наукової роботи.

У висновках стисло сформульовано основні наукові та практичні результати дисертаційної роботи.

У додатках містяться акти впровадження результатів дисертаційної роботи та лістинг (початковий код) програмної моделі системи

Таким чином, усі положення, винесені на захист, висвітлені в тексті дисертації. Зміст дисертаційної роботи відповідає її назві. Дисертація написана науковою мовою та оформлена відповідно до існуючих нормативних документів.

7. **Рекомендації щодо використання результатів дисертації.**

Запропоновані в роботі моделі, методи та алгоритми можуть бути використані для побудови високоефективної системи виявлення вторгнень, яка є

складовою комплексної системи захисту інформаційних ресурсів від кібератак.

8. **Повнота викладення основних результатів дисертації**.

Основні результати дисертації достатньо повно відображені в 57 наукових працях (в авторефераті наведено 42), серед яких монографії, статті у наукових виданнях, що входять до переліку фахових видань України з технічних наук та індексуються в міжнародних науково-метричних базах, та пройшли апробацію на багатьох всеукраїнських та міжнародних науково-технічних конференціях.

9. **Автореферат дисертації**

Автореферат дисертації за своїм змістом повністю відповідає дисертаційній роботі.

10.**Зауваження щодо змісту і оформлення дисертації.**

1. У першому розділі дисертації після проведеного аналізу відомих систем виявлення вторгнень наведено такий висновок: «…сучасні СВВ аномального принципу, в основному, засновані на математичних моделях, що потребують багато часу для отримання статистичних даних, реалізацію процесу навчання (в основному для нейромережевих систем) та здійснення інших складних і довготривалих підготовчих процедур». При цьому всі використані оцінки характеристик мають якісний, а не кількісний характер. Багато часу для деяких систем це доба, а для інших – місяць. Тому доцільно було б навести конкретні приклади з кількісними характеристиками. Крім того, тривалість підготовчих процедур не впливає суттєво на тривалість створення системи.

2. Аналізуючи відомі системи виявлення вторгнень і математичні моделі, покладені в їх основу, автор відзначає, що «… в жодній з проаналізованих систем не використовуються методи нечітких множин, які показали свою ефективність при вирішенні такого класу задач». Було б доцільно навести конкретні приклади, а не обмежуватися лише посилання на публікації.

3. Не зрозуміло, чому для опису складових кортежної моделі формування атакуючих середовищ автор використовує одночасно три мови. Наприклад, кібератаки з іменами: «Сніффінг (Sniffing (SNF))», «Відмова в обслуговуванні (Denial of service (DS))»;ІД параметрів: «Кількість вхідних пакетів в мережі» або «Количество входных пакетов в сети (КВП)», «Швидкість обробки пакетів на стороні одержувача» або «Скорость обработки пакетов на стороне получателя (СОП)», «Кількість одночасних підключень до серверу» або «Количество одновременных подключений к серверу (КОП)»; ІД лінгвістичних оцінок (суджень) експерта: «Дуже мале» або «Очень малое (ОМ)», «Мале» або «Малое (М)», «Велике» або «Большое (Б)».

4. Описуючи структуру системи виявлення кібератак (рис. 5.1). автор не пояснює, які саме методи використовуються для узгодження параметрів баз даних кібератак (БДК), правил (БДП) і еталонів (БДЕ).

5. Оскільки в роботі декларується, як один із результатів, можливість виявлення нових видів кібератак за максимально короткий час, то доцільно було б навести оцінки тривалості процесу ініціалізації БД і процесу виявлення кібератак. Наявність таких оцінок надала б можливість порівняти за цією характеристикою запропоновану автором і відомі системи.

6. Автор не пояснює, яким чином буде виявлено нову кібератаку, якщо вона не буде змінювати параметри, аналіз яких передбачено в системі.

7. В авторефераті та дисертації зустрічаються стилістичні, синтаксичні та граматичні помилки.

11. Загальна оцінка дисертації

Оцінюючи роботу в цілому, вважаю, що в дисертації отримано нове рішення важливої науково-прикладної проблеми, пов'язаної з побудовою систем виявлення аномальних станів, породжених реалізацією нових типів загроз.

Дисертація є завершеною науково-дослідною роботою. Вважаю, що за актуальністю вибраної теми, обсягом і рівнем виконаних теоретичних і експериментальних досліджень, достовірністю і обґрунтованістю висновків, новизною досліджень, значенням отриманих результатів для науки і практики дисертаційна робота задовольняє вимогам п. 9, 10, 12 «Порядку присудження наукових ступенів», затвердженого Постановою КМУ від 19 серпня 2015 року № 656, а її автор, Корченко Анна Олександрівна, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
завідувач кафедри захисту інформації
Вінницького національного
технічного університету,
д.т.н., професор В.А. Лужецький

"20" червня 2019 р.

Підпис Лужецького В.А
ПОСВІДЧУЮ
Зав. канцелярією