Голові спеціалізованої вченої ради Д 26.185.01
Інституту проблем моделювання в енергетиці
ім. Г.Є. Пухова НАН України
03164, Київ-164, вул. Генерала Наумова, 15

ВІДГУК
офіційного опонента на дисертаційну роботу
ПОТЕНКА ОЛЕКСАНДРА СЕРГІЙОВИЧА
«Методи визначення функціонального профілю захисту автоматизованої системи з урахуванням поточного рівня загроз»,
яка подається на здобуття наукового ступеня
кандидата технічних наук за спеціальністю
05.13.21 – системи захисту інформації

Дисертаційна робота Потенка О.С. присвячена вирішенню актуального наукового завдання, що полягає у розробленні методів визначення функціонального профілю захищеності автоматизованої системи з урахуванням поточного рівня загроз за рахунок аналізу цільової функції за Беллманом та виміру математичного сподівання успішної протидії.

1. Актуальність роботи

Необхідність захисту інформації призводить до створення повного життєвого циклу (проектування, виробництво, експлуатація) захищених автоматизованих систем (АС), призначених для накопичення, обробки, зберігання та передавання інформації, що потребує захисту.

Існуючі нормативні документи технічного захисту інформації (НД ТЗІ) слугують для визначення функціонального профілю захищеності (ФПЗ) оброблюваної інформації шляхом стандартизації необхідних рівнів послуг, які повинен реалізовувати комплекс засобів захисту, щоб задовольняти певні вимоги щодо захищеності інформації. Надалі цей профіль підлягає оцінюванню та визначенню відповідності наданих послуг встановленим вимогам. Значне зростання нових загроз вимагає розвинення як правової бази, так і наукового забезпечення для вирішення відповідних проблем.

Для забезпечення необхідного рівня захищеності інформації в АС створюються комплексні системи захисту інформації (КСЗІ). Так, відповідно до закону України «Про захист інформації в інформаційно-комунікаційних системах», державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися

в системі із застосуванням КСЗІ з підтвердженою відповідністю. Підтвердження відповідності КСЗІ здійснюється за результатами державної експертизи, яка проводиться з урахуванням галузевих вимог та норм інформаційної безпеки у порядку, встановленому законодавством.

На практиці, під час проведення експертиз КСЗІ експерт аналізує механізми захисту, реалізовані в системі. Його завданням є виявлення цих механізмів, перевірка їх працездатності, коректності реалізації та достатності для протидії існуючим загрозам. ФПЗ ж визначають на етапі розробки технічного завдання. Його формують на основі політик безпеки, моделі порушника та моделі загроз. За цих обставин розробник системи стикається з проблемою створення переліку рівнів послуг, які повинні реалізовувати засоби захисту інформації для забезпечення визначених вимог щодо її захищеності. Очевидно, що створення профілю захищеності з максимально можливим набором рівнів послуг в більшості випадків не є економічно вигідним. Як результат, виникає потреба в визначенні профілю захищеності з мінімально необхідним рівнем послуг, який є достатнім для забезпечення визначених вимог щодо захищеності інформації. Оскільки за типових умов кількість можливих варіантів профілів може досягати 15 мільярдів, повний їх перебір є неефективним.

Таким чином, дисертаційне дослідження Потенка Олександра Сергійовича, спрямоване на визначення та оцінювання ФПЗ АС з урахуванням поточного рівня загроз, є актуальним.

2. Структура та зміст роботи

У **вступі** представлено актуальність теми, розглянуто зв'язок роботи з науковими програмами та темами, визначено мету та завдання дослідження, описано методи дослідження, висвітлено наукову новизну та практичне значення отриманих результатів, зазначено особистий внесок автора в працях, опублікованих у співавторстві, наведено інформацію про апробацію результатів і їх впровадження, а також представлено список публікацій за темою роботи.

Розділ 1 присвячено дослідженню та аналізу небезпек у інформаційному забезпеченні кібероб’єктів, що відповідають за функціонування різних технологічних процесів.

Зокрема, в підрозділі 1.1 проведено аналіз, систематизацію та формалізацію міжнародних критеріїв безпеки комп'ютерних систем. Підрозділ 1.2 присвячено аналізу вітчизняних критеріїв оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99. У підрозділі 1.3 проведено порівняльний аналіз методів визначення ФПЗ АС від несанкціонованого доступу. Перший розділ завершується підрозділом 1.4, у якому викладено висновки, де зазначено, що незважаючи на наявність низки методів визначення ФПЗ АС, кожен з них має свої недоліки, а, відтак, дисертаційна робота є актуальною.

Розділ 2 присвячено визначенню профілів протидії загрозам на основі динамічного програмування з використанням оптимального принципу Беллмана. У підрозділі 2.1 наведено теоретичні принципи динамічного програмування. У підрозділі 2.2 розглянуто задачі оптимізації за Беллманом, зокрема використання детермінованих методів розв'язання для розподілу однорідних ресурсів. У підрозділі 2.3 автором запропоновано новий метод оцінювання та оптимізації інформаційної безпеки АС за мультикритерієм «ризик безпеки – гарантія безпеки – вид інформаційної діяльності – вартість». У підрозділі 2.4 автором запропоновано вимоги щодо алгоритмічної реалізації визначення профілю протидії загрозам. У підрозділі 2.5 сформовано висновки до другого розділу.

Розділ 3 присвячено алгоритмічній реалізації методів визначення ФПЗ. У підрозділі 3.1 автором розроблено алгоритм для ефективної перевірки збіжності методу для проектування адаптивних профілів для підкласів АС. Після цього проведено тестовий розрахунок для перевірки коректності реалізації, результати якого використано в четвертому розділі. Перевірено та підтверджено працездатність методу з урахуванням обмежень. У підрозділі 3.2 розроблено алгоритм визначення ФПЗ АС для профілю захищеності з урахуванням рівня загроз для підкласів К, Ц, Д, КЦ, КД, ЦД, КЦД. Алгоритм має параметр $n = 67$, що відповідає кількості стандартних послуг безпеки, та інші значення p_i, a_i, w_i відповідно до методики проектування профілів для АС-1, АС-2, АС-3. Крім того, в алгоритмі змінюються критерії зупинки та стратегія пошуку. У підрозділі 3.3, спираючись на попередні алгоритми та враховуючи можливості сучасних систем підтримки прийняття рішень, визначено вимоги до програмної реалізації програмного застосунку. У підрозділі 3.4 сформульовано висновки до розділу 3.

У розділі 4 описано програмну реалізацію методів визначення ФПЗ. У підрозділі 4.1 описано програмну реалізацію тестового алгоритму для перевірки збіжності метода. Підрозділ 4.2 описує розроблену автором програмну реалізацію методу визначення ФПЗ АС, яка використовує математичний метод динамічного програмування для «генерації» профілів протидії загрозам порушення конфіденційності К, цілісності Ц, доступності Д і спостережності Н інформації АС за підкласами К, Ц, Д, КЦ, КД, ЦД, КЦД. У підрозділі 4.3 наведено результати тестування програмного модуля для перевірки збіжності методу визначення ФПЗ, а також порівняння для різних підкласів систем. Наведено порівняльний аналіз запропонованого методу визначення ФПЗ АС з іншими методами побудови ФПЗ. Етапи створення КСЗІ відповідно до НД ТЗІ 3.7-003-2005 описано в підрозділі 4.4., після чого наведено приклади державних експертиз КСЗІ, в яких використовувались напрацювання автора. У підрозділі 4.5 сформульовано висновки до розділу 4.

У висновках наведено основні результати дисертаційного дослідження, наукову та практичну цінність отриманих результатів.

Додатки містять документи, що підтверджують результати дисертаційного дослідження.

3. Ступінь обґрунтованості наукових положень, висновків і рекомендацій

Наукові положення та висновки, представлені в дисертації, мають достатнє обґрунтування. Методи дослідження, які використовуються в роботі (системний і функціональний аналіз, математичне моделювання, теорія ймовірностей та математична статистика, теорія ризиків, теорія алгоритмів, теорія баз даних, об'єктно-орієнтоване програмування, методи оптимізації, планування наукового експерименту та обробки його результатів) застосовані належним чином. Достовірність теоретичних результатів перевірено експериментально та підтверджено відповідними актами впровадження.

4. Достовірність результатів досліджень

Достовірність результатів дисертаційного дослідження забезпечено коректною постановкою задач з урахуванням відповідних обмежень, застосуванням сучасних математичних методів, узгодженням результатів з експериментальними даними та апробацією основних результатів на наукових конференціях. Отримані результати є обґрунтованими, достовірними та новими.

Ознак академічного плагіату, фабрикації, фальсифікації, некоректно оформлених запозичень чи інших ознак неправомірного використання результатів інших авторів без зазначення авторства в роботі не виявлено. Використані ідеї та результати інших авторів мають належні посилання на джерела.

5. Наукова новизна дисертаційної роботи полягає в наступному:

У роботі вирішено актуальне наукове завдання розроблення методів визначення ФПЗ для різних класів АС, зокрема:

1) запропоновано критерії визначення ФПЗ, які за рахунок аналізу цільової функції за Беллманом та визначення математичного сподівання успішної протидії окремої функціональної послуги безпеки, дозволяють у формальному вигляді сформувати необхідний набір послуг безпеки для реалізації процесу вибору рівня захисту;

2) вдосконалено метод визначення ФПЗ для різних класів АС, який за рахунок використання розподілу однорідних ресурсів дозволяє автоматизувати процес генерування ФПЗ та порівняння його з відповідним рівнем захисту;

3) запропоновано підхід до перевірки збіжності методу визначення ФПЗ для різних класів АС, який за рахунок автоматизації процесу адаптації загрозам за підкласами АС дозволяє зменшити кількість помилок при складанні ФПЗ;

4) запропоновано метод визначення ФПЗ для різних класів АС, який, за рахунок окремої оцінки умовного рейтингу та коефіцієнту вагомості, дозволяє зменшити час при складанні ФПЗ для різних класів АС.

6. Практичне значення результатів дисертаційного дослідження

Серед практичного значення отриманих результатів варто виділити те, що на базі запропонованого методу визначення ФПЗ для різних класів АС розроблено алгоритмічне забезпечення, яке дозволяє створювати відповідний програмний продукт.

На основі запропонованого алгоритму реалізовано програмний застосунок, який можна використовувати для перевірки ФПЗ для різних класів АС за мультикритерієм «ризик безпеки – гарантія безпеки – вид інформаційної діяльності – вартість», що суттєво зменшує час для побудови комплексної системи захисту інформації та для проведення експертиз систем технічного захисту інформації КСЗІ.

Результати дисертаційного дослідження впроваджено у діяльність ТОВ «Інформаційна безпека» та ДП «Державний науково-технічний центр з ядерної та радіаційної безпеки».

7. Повнота викладення результатів у опублікованих матеріалах

Основні положення і результати дисертаційного дослідження опубліковано в 33 наукових працях, серед яких: 1 стаття в науковому періодичному виданні, що індексується наукометричною базою даних Scopus, 11 статей у наукових фахових виданнях України, 20 праць опубліковано в матеріалах міжнародних і всеукраїнських наукових і науково-практичних конференцій, 1 свідоцтво про реєстрацію авторського права на твір. У опублікованих працях повністю представлено основні наукові положення дисертаційної роботи та отримані результати. Рівень і кількість публікацій відповідають вимогам, що ставляться до кандидатських дисертацій в Україні.

8. Автореферат повністю відображає основні положення дисертаційної роботи і детально висвітлює актуальність, мету та завдання дослідження, основні наукові положення, практичну цінність, апробацію дисертації, її структуру за розділами та висновки. Дисертаційну роботу та автореферат оформлено відповідно до вимог Міністерства освіти і науки України для кандидатських дисертацій.

9. Зауваження до дисертаційної роботи:

1. У першому розділі дисертації варто було більше уваги приділити аналізу методів визначення ФПЗ АС від несанкціонованого доступу, ніж критеріям безпеки комп'ютерних систем. У вступі ж доцільно було

конкретизувати, які методи досліджень використано для вирішення кожного з основних наукових завдань роботи.

2. Дисертація містить різні формулювання одних і тих самих об’єктів (профіль захисту – профіль захищеності – профіль безпеки; множина критеріїв – мультикритерій; метод визначення функціонального профілю – метод оцінки та оптимізації інформаційної безпеки тощо) без попереднього визначення та обґрунтування, що ускладнює розуміння матеріалу.

3. У тексті роботи відсутнє формалізоване представлення підходу до перевірки збіжності методу визначення ФПЗ для різних класів АС, а також розробленого методу визначення ФПЗ для різних класів АС, що ускладнює можливість їх аналізу. Крім того, було б корисно більш детально описати ступінь новизни та досягнутий ефект у порівнянні з існуючими аналогами.

4. У підрозділах 3.1 і 3.2 блок-схеми тестового алгоритму перевірки збіжності та робочого варіанту алгоритму визначення ФПЗ АС представлено в спрощеному вигляді. Загалом, це дозволяє оцінити їхню структуру, проте для повного розуміння алгоритмів, а також для повторного їх відтворення доцільно було б їх деталізувати.

5. У тексті дисертації й авторефераті відсутні пояснення та обґрунтування (вид і умови експерименту, методи опрацювання результату тощо) стосовно кількісних показників отриманого позитивного ефекту від застосування підходу до перевірки збіжності методу визначення ФПЗ для різних класів АС (зменшення обсягу розрахунку до 10,45% від максимального), а також від застосування розробленого методу визначення ФПЗ для різних класів АС (зменшення часу при складанні ФПЗ на 15%).

6. У підрозділі 4.3 наведено графіки математичного сподівання успішного захисту для підсистем різних класів, але, оскільки розрахунки майже не відрізняються, то отримані графіки важко сприймати візуально. Зважаючи на те, що вказані залежності несуть важливий зміст для оцінювання ефективності запропонованих автором рішень, варто було б знайти більш зручний спосіб їх представлення.

7. У авторефераті не збалансовано обсяги представлення основних наукових результатів дисертаційного дослідження. Так, для розкриття змісту пунктів 1, 2, 4 наукової новизни використано загалом до 3 сторінок автореферату. Для кращого представлення отриманих наукових результатів цей обсяг доцільно було збільшити.

8. Дисертація містить синтаксичні, пунктуаційні, стилістичні помилки.

Зазначені зауваження не є критичними та не впливають на загальну позитивну оцінку роботи.

10. Висновки

Дисертаційна робота Потенка Олександра Сергійовича «Методи визначення функціонального профілю захисту автоматизованої системи з

урахуванням поточного рівня загроз», яка подана на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації, є завершеною працею, в якій вирішено актуальне наукове завдання розроблення методів визначення функціонального профілю захисту для різних класів автоматизованих систем та отримано нові науково обґрунтовані результати.

Робота задовольняє вимогам, які висуваються до дисертаційних робіт на здобуття наукового ступеня кандидата технічних наук, а її автор, Потенко Олександр Сергійович, заслуговує на присудження наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент
проректор з науково-дослідної роботи
та міжнародних зв'язків
Черкаського державного
технологічного університету,
д.т.н., професор Еміль ФАУРЕ

15 серпня 2024 р.

Вчений секретар