МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

СУЛІМА Олександр Андрійович

УДК 004.056.52

МЕТОДИ ОРГАНІЗАЦІЇ ЗАХИСТУ ДОСТУПУ ДО ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ ВИКОРИСТАННЯ БАГАТОРІВНЕВИХ МОДЕЛЕЙ

05.13.21 – «Системи захисту інформації»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2017

Дисертацією є рукопис.

Робота виконана в Інституті проблем моделювання в енергетиці ім. Г. Є. Пухова Національної академії наук України.

Науковий керівник:	кандидат технічних наук, с.н.с. **Давиденко Анатолій Миколайович,** Інститут проблем моделювання в енергетиці ім. Г. Є. Пухова НАН України, в.о. заст. директора з науково-організаційної роботи.
Офіційні опоненти:	доктор технічних наук, доцент **Терейковський Ігор Анатолійович,** Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри системного програмування і спеціалізованих комп'ютерних систем; кандидат технічних наук **Гізун Андрій Іванович,** Національний авіаційний університет, доцент кафедри безпеки інформаційних технологій.

Захист відбудеться « 30 » листопада 2017 р. о 16 ^{00} годині на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, Київ, пр. Космонавта Комарова, 1, аудиторія 11-111.

З дисертацією можна ознайомитись в науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, Київ, пр. Космонавта Комарова, 1.

Автореферат розісланий «____» жовтня 2017 р.

В.о. ученого секретаря
спеціалізованої вченої ради
д.т.н., професор В. В. Козловський

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність. Проблеми захисту та оцінки даних інформаційних систем на даний час продовжують залишатися надзвичайно актуальними. Особливо важливими є завдання, пов'язані з оцінкою та захистом даних у системах, орієнтованих на співпрацю з обраними об'єктами та відповідними середовищами. Головна мета захисту інформаційних даних полягає у тому, щоб виключити можливість їх несанкціонованого використання або втрат у відповідному середовищі. Важливим напрямом протидії таким ситуаціям є метод, який полягає у захисті даних шляхом надання останніх тільки тим користувачам, які мають відповідний допуск. Такий метод ґрунтується на реалізації різних способів оцінки даних, на основі яких приймаються рішення про їх надання чи не надання конкретному користувачу. Очевидно, що в рамках реалізації цього методу необхідно і важливо контролювати користувача, який має право на використання тих чи інших даних з відповідних інформаційних систем. Розпізнавання користувачів полягає у визначенні допуску конкретного користувача та його повноважень на отримання і використання відповідних даних. Зазначені аспекти приведеної проблеми розв'язують системи доступу до даних, за якими звертаються користувачі.

Іншою складовою цієї проблеми є оцінка даних, яка визначає необхідний рівень їх захисту та може умовно називатися рівнем конфіденційності. Рівень конфіденційності є основним чинником для прийняття інформаційною системою рішення про надання чи не надання відповідних даних користувачу, який звернувся за їх отриманням.

На сучасному етапі розвитку інформаційних систем оцінка рівня конфіденційності, на відміну від минулих уявлень, не є сталою, навіть у випадку, коли одночасно з декларацією рівня конфіденційності декларується період, протягом якого відповідна оцінка повинна зберігатися. Ці оцінки змінюються з часом під впливом різних факторів, що характеризують середовище, до якого відносяться відповідні дані. Такі зміни можуть призводити до зміни рівня повноважень користувачів.

Наведені аспекти ілюструють складність задач, пов'язаних з оцінкою даних і, відповідно, з рівнем їх захисту та реалізуються через управління доступу до них користувачів, які мають різні права на використання таких даних. У зв'язку з цим задачі, що досліджуються та розв'язуються у дисертаційній роботі, є важливими та актуальними для подальшого практичного впровадження.

Аналогічними проблемами займається ряд відомих вчених, зокрема: Д. Белл, Л. Лападула, А. Йонез, Р. Ліптон, І. Снайдер, Л. Діон, Р. Сандху, Е. Койн, А. Файнстайн, К. Йомен, К. Ландвер, К. Хайтмайер, Дж. Маклін, Д. Кларк, Д. Уілсон, Дж. Міллен, К. Біба, М. Харрісон та інші.

Беручи до уваги наведене вище, є підстави вважати, що тема дисертаційної роботи є новою та актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Робота виконувалася у рамках замовлень наукових досліджень Президії Національної академії наук України в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова (ІПМЕ): «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики» (шифр МОД-Д, реєстраційний номер 0114U002361, 2014-2017 рр.).

Мета і задачі дослідження. Мета роботи полягає у вирішенні науково-прикладної задачі, спрямованої на побудову інформаційних засобів для реалізації методів підвищення рівня захисту даних в інформаційних системах на засадах використання багаторівневої системи надання повноважень та застосування автоматизованого процесу визначення поточних значень рівня конфіденційності даних. Зазначене

дозволяє забезпечити необхідну зміну рівня їх конфіденційності в процесі функціонування інформаційних систем. Для досягнення поставленої мети **необхідно було розв'язати наступні задачі:**

– здійснити аналіз існуючих методів надання повноважень користувачам на використання даних з інформаційних систем, за підсумками чого визначити необхідність подальших досліджень, пов'язаних з методами надання повноважень на використання даних різних рівнів конфіденційності;

– розробити метод формального опису параметрів, що характеризують моделі даних інформаційної системи;

– розробити метод оцінки параметрів інформаційних запитів задач, що представляють собою дані, які знаходяться в системі захисту, що функціонує в рамках інформаційної системи;

– визначити компоненти моделі багаторівневої системи доступу;

– розробити метод визначення параметрів додаткових компонентів системи доступу, що дозволить керувати процесом доступу до інформаційної системи;

– розробити алгоритм реалізації основних процесів, що функціонують в системі доступу до інформаційної системи;

– розробити алгоритм загальної організації роботи дворівневої системи доступу до даних.

Об'єктом досліджень є організація процесу доступу до інформаційних ресурсів.

Предметом досліджень є методи доступу до інформаційних ресурсів.

Методи дослідження. Для розв'язання задач побудови багаторівневих моделей, формування рішень про надання повноважень використовувалися методи математичної логіки і семантичного аналізу, комп'ютерне моделювання та теорія інформаційних систем.

Наукова новизна отриманих результатів. У дисертаційній роботі розв'язана та досліджена нова науково-прикладна задача, що полягає у розробці та дослідженні методів захисту даних у спеціалізованих інформаційних системах від несанкціонованого доступу на основі використання багаторівневої моделі доступу та методу оцінки рівня їх захисту.

Наукова новизна отриманих результатів полягає в наступному:

– *удосконалено* метод формального опису параметрів інформаційних моделей даних, які за рахунок обчислення таких величин дозволяють більш повно їх оцінювати, співставляючи з необхідними рівнями захисту;

– *вперше розроблено* метод визначення параметрів інформаційних запитів задач та їх оцінок, який на основі використання характеристик конфіденційних даних з інформаційної системи, незалежно від користувача, що представив відповідну задачу, дозволить приймати рішення системою про надання повноважень передачі задачі відповідних даних, при цьому стає можливим уникнути небезпек у результаті впливу суб'єктивних факторів користувача;

– *вперше розроблено* метод визначення параметрів додаткових компонентів засобів доступу до інформаційної системи, який за рахунок аналізу предметної області, що обслуговується інформаційною системою, дозволяє співставити рівень конфіденційності даних з величинами параметрів, які зазначені в інформаційному запиті задачі, яка звернулася із запитом, що дає змогу встановити залежність між рівнем захисту системи та умовами предметної області з використання результатів розв'язання прикладних задач;

– *вперше розроблено* основні компоненти дворівневої моделі доступу до даних, у якій відповідні рівні функціонують незалежно, але при переході з нижчого рівня на вищий також враховується результати перевірок нижчого рівня, за рахунок чого з'являється можливість уникнути впливу нижчого рівня на вищий при розв'язанні задач доступу до інформаційного ресурсу, що дозволяє надання інформації з високим рівнем конфіденційності узалежнити від цілі розв'язання задачі та узалежнити від характеру впливу використання цього розв'язання в предметній області, яку обслуговує інформаційна система.

Практичне значення результатів та їх впровадження. Отримані в дисертаційній роботі результати використовувалися для створення алгоритмів та реалізації програмних засобів, розв'язання задач захисту конфіденційних даних з різним рівнем конфіденційності, які забезпечують необхідний рівень захисту в процесі функціонування інформаційної системи.

Практична цінність роботи полягає в наступному:

– на основі запропонованої дворівневої моделі захисту даних розроблено алгоритм, який реалізує процес надання повноважень задачам, що звертаються за конфіденційними даними та розроблено відповідну блок-схему;

– на основі запропонованих елементів засобів доступу до інформаційної системи розроблено алгоритм загальної організації роботи дворівневої системи доступу до даних, що забезпечує елімінацію суб'єктивних факторів користувача, які могли б впливати на можливість доступу до конфіденційних даних.

Розроблені методи організації доступу до даних використовувалися в Інституті кібернетики ім. В. М. Глушкова НАН України при проведенні первинної державної експертизи, що дозволило використовувати системи оцінювання ризиків безпеки інформаційних ресурсів в умовах великих обсягів консолідованої інформації та підвищити ефективність і рівень автоматизації процесів управління ризиками при побудові комплексних систем захисту інформації та систем менеджменту інформаційної безпеки.

Результати дисертаційної роботи впроваджено до навчального процесу НАУ і використовуються на кафедрі БІТ під час викладання дисципліни «Управління інформаційною безпекою».

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виноситься до захисту, отримано автором самостійно. У роботі [3], опублікованій у співавторстві, автору належить аналіз методів та засобів опису процесів надання повноважень.

Апробація результатів дисертаційної роботи. Основні наукові результати та положення дисертаційної роботи доповідалися на міжнародних і національних науково-технічних конференціях та семінарах, зокрема: «Моделювання: XXXIV» науково-технічна конференція (Київ 2015 р.); «Фундаментальні та прикладні дослідження у сучасній науці» IV наукова конференція (Харків 2016 р.); «Моделювання: XXXV» науково-технічна конференція (Київ 2016 р.); «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» міжнародна наукова конференція (Тернопіль 2017 р.).

Публікації. Основний зміст дисертаційної роботи викладено в 11 наукових працях, серед яких шість статей надруковано у фахових виданнях України; дві увійшли до наукометричної бази даних Index Copernicus [3, 6], п'ять тез та матеріалів у збірниках наукових конференцій.

Структура та обсяг дисертації. Дисертаційна робота складається з вступу,

чотирьох розділів, висновків, списку використаних джерел та додатків. Роботу викладено на 193 сторінках, які містять 164 сторінки основного тексту, дві таблиці, 11 рисунків, перелік використаних джерел з 132 найменувань та три додатки.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі викладено узагальнений зміст дисертаційної роботи, обґрунтовано її актуальність, сформульовано мету та методи вирішення відповідних задач, а також відображено наукову новизну і практичну цінність отриманих результатів.

Таблиця 1

Результати аналізу основних систем та моделей надання повноважень

MC	*Q*	*W*	*E*	*R*	*T*	*Y*
Белла-Лападула	R	-	-	Z	-	-
Довірених суб'єктів	R	-	+	X	-	-
Розподілених систем	R	-	+	C	-	-
Адепт-50	R	-	-	C	-	-
LWM	R	-	+	Z	-	-
Лендвера	R	-	+	V	-	-
MAC	R	+	+	X	-	-
HRU	R	+	-	B	-	-
Кларка-Вілсона	R	-	-	Z	-	-
Міллена (MPP)	R	-	+	Z	-	-
MMS	R+	+	+	M	-	-
Біба	R-	-	-	N	-	-
Багаторівнева система доступу	R+	+	+	M	+	+

У першому розділі проаналізовано відомі методи надання повноважень користувачам інформаційних систем та проведено аналіз відповідних основних систем. Дані, що зберігаються в інформаційній системі, характеризуються різними параметрами, один з яких представляє собою параметр рівня їх конфіденційності, що характеризує необхідний рівень їх захисту. Найбільш поширеною моделлю доступу є матрична модель доступу, в якій у першому стовпці матриці розміщуються користувачі, яких прийнято називати суб'єктами, а в першому рядку матриці розміщуються ідентифікатори даних чи їх груп, які називаються об'єктами. У роботі проводиться аналіз методів оцінок рівня безпеки доступу до даних. Досить поширеною оцінкою величини зміни рівня безпеки інформаційної системи є величина ризику того, що рівень безпеки зменшиться. При відповідній інтерпретації елементів, що входять до моделі ризику Ru, стає можливим визначити величину, яка інтерпретує зниження рівня безпеки R у системі. Наступний підхід до оцінки рівня безпеки грунтується на використанні експертних даних про параметри, що використовуються для визначення величини ризику.

Існує велика кількість моделей систем надання повноважень користувачам. Їх різноманіття визначено різницею в цілях і підходах до реалізації розподілу прав доступу. Критеріями вибору використання того чи іншого підходу є вимоги з безпеки і вартості процедури обробки інформації для конкретного функціонального призначення, яка визначена цільовою предметною областю, і відповідно, застосуванням того чи іншого рішення для реалізації інформаційних технологій. Проаналізовано основні найбільш поширені моделі надання доступу користувачам та їх ключові властивості, результати яких приведено у табл. 1: MC – модель конфіденційності; HRU – модель Харрісона-Руззо-Ульмана; LWM – модель Low-Water-Mark; MZD – модель динамічної системи захисту доступу; MAC – модель мандатного доступу; Q – типи доступу, що використовуються в моделі; W – системний компонент; E – компонент безпеки; R – особливості операцій доступу суб'єкта до об'єктів; R– read, write; R+ – read, write, create, delete, операції з об'єктами

специфічної структури; R- і Z – обмеження накладаються на найпростіші операції read, write; X – операції read, write можуть бути видаленими; C – забезпечує однорідний контроль права на доступ над неоднорідними множинами програм і даних, файлів, користувачів; V – частина цих обмежень повинна реалізовуватися користувачами системи, а частина системою; B – містить тільки одну умову; N – множини суб'єктів і об'єктів упорядковані відповідно до рівнів безпеки; M – крім найпростіших операцій у моделі можуть з'явитися операції, спрямовані на специфічну обробку інформації; L – наявність ієрархії рівнів доступу, орієнтованих окремо на користувача і задачу; T – можливість отримання частки інформації з консолідованого блоку більш високого рівня конфіденційності; Y – дробове представлення способу доступу.

Результати аналізу основних систем та моделей надання повноважень користувачам, що наведено у таблиці 1, свідчать про переваги запропонованої багаторівневої системи доступу перед іншими. Зокрема, наявність ієрархії рівнів доступу, орієнтованих окремо на користувача і задачу; можливість отримання частки інформації з консолідованого блоку більш високого рівня конфіденційності та дробове представлення способу доступу.

Проведений аналіз свідчить, що задача побудови нових методів організації доступу до даних користувача, які підвищували б рівень захисту даних інформаційної системи від несанкціонованого їх використання, є актуальною.

У другому розділі досліджуються методи формального опису параметрів процесів надання повноважень та фактори, що на них впливають. Перший фактор визначає рівень залежності між рівнем конфіденційності даних та кількістю користувачів(h_i), які такими даними (x_i) користуються. Рівень конфіденційності даних позначимо $r_i(x_i)$. Тоді можна *вважати*, що $r_i(x_i)$=$k_{Rz}/mh_i(\alpha_i)$, де α – власний рівень безпеки h_i, m – кількість користувачів. Другий фактор визначає зміну рівня конфіденційності, який з часом зменшується. Якщо x_i використовується часто, то таке зменшення $r_i(x_i)$ відбувається швидше. Якщо x_i взагалі не використовується, то зміна значення $r_i(x_i)$ може відбутися через певний проміжок часу, що описується наступними співвідношеннями:

$\{(m(x_i)=0)\&(\delta t_i(x_i)) \geq \Delta T_i(x_i)\} \rightarrow [(r_i(x_i)=0)\&(x_i \notin IS)]$,

$[(m(x_i)/\Delta t) \rightarrow 0] \rightarrow [r_i(x_i) \rightarrow min\, r_i(x_i)]$.

Введемо наступні положення та визначення.

Положення 1. Рівень конфіденційності відповідних даних x_i з часом зменшується незалежно від інтенсивності використання x_i для розв'язання задач.

Визначення 1. Важливістю даних x_i будемо називати параметр, що характеризує частоту використання даних за період часу, протягом якого відповідні дані використовуються, що описується співвідношенням:

$\aleph(x_i)$=$[m_j(x_i)/\Delta t_j] + \sum_{j=1}^{N} \Delta t_j$, де $\aleph(x_i)$ – значимість даних, що ідентифікуються змінною x_i ; m_j – кількість запитів на використання даних x_i за встановлений проміжок часу Δt_j; N – деяке число $N > n$, де n – довільне ціле число, що визначає кількість Δt_jта відповідає часу, протягом якого використовується x_i.

Визначення 2. Рівень конфіденційності $r_i(x_i)$ даних x_i зв’язаний з рівнем небезпеки, до якої може призвести несанкціоноване використання x_i під час розв’язання задачі $Za_i(x_i)$.

Розглянемо визначення параметрів інформаційних запитів прикладних задач та методи їх оцінок. За рахунок параметрів інформаційних запитів задачі, яку представив

користувач, стало можливим для систем надання повноважень (SNP) надавати повноваження задачі на використання конфіденційних даних незалежно від можливого впливу користувача на відповідне рішення системи надання повноважень.

Метод формального опису даних реалізується наступними етапами.

На першому етапі система надання повноважень використовує наступні дані задачі: ціль розв'язання задачі $C(Za_i)$; наявність повноважень у h_i на розв'язання задачі (Za_i); параметри задачі, зовнішні засоби, які повинна використовувати задача Za_i в процесі розв'язання.

Повноваження користувача $p(h_i)$, що характеризують задачу, визначаються наступними параметрами: рівнем конфіденційності задачі $r_i(Za_i)$; рівнем значимості задачі $\aleph_i(Za)$; параметрами, що характеризують ціль задачі $p[C(Za_i)]$; рівнем актуальності задачі для предметної області її інтерпретації (W_i); кількістю конфіденційних даних, що використовуються в задачі $kr_i(x_1, \dots, x_n)$, що можна записати, як: $p(z_i) = f\{r_i(Za_i), p[C(Za_i)], \aleph_i(Za_i), A[Z_i(W_i)], kr_i(x_1, \dots, x_n)\}$.

Етап 1. Прийняття рішень про надання повноважень: $SNP \rightarrow C(Z_i); h_i \rightarrow Z_i$; параметри Z_i; зовнішні засоби $Z_i.p(z_i) = f\{r_i(Za_i),\ p[C(Za_i)],\ \aleph_i(Za_i),\ A[Z_i(W_i)],\ kr_i(x_1, \dots, x_n)\}$.

Етап 2. Аналіз суперечностей: An_i-? $\rightarrow$ W_iR -?

Етап 3. Аналіз можливостей розширення системи: $R = \{r_1, \dots, r_m\}$ така, що $\{r_1 < r_2 < \dots < r_m\}$, то система R може бути розширена $r_{m+t} > r_m$.

Етап 4. Аналіз функціональних можливостей та методу оцінки окремих компонентів засобів захисту:

$\{SD[K(p_1^k, \dots, p_r^k)]\&ZD[p_1^{SD}, \dots, p_l^{SD}] \rightarrow Al^D(p_1^k, \dots, p_r^k, p_1^{ID}, \dots, p_e^{IO})\} \rightarrow 1 \rightarrow \{[(K \rightarrow SK)\&(K \rightarrow \neg NK)] \vee [(K \rightarrow NK)\&\neg(K \rightarrow SK)]\};$

$\{[K(p_1^k, \dots, p_r^k)]\&Za_i[p_1^Z, \dots, p_l^Z] \rightarrow ZD \rightarrow Al^D(p_1^k, \dots, p_r^k, p_1^{ID}, \dots, p_e^{ID})\} \rightarrow\rightarrow \{SK[Za_i[p_1^Z, \dots, p_l^Z] \rightarrow SNP \rightarrow Al^{ND}(p_1^Z, \dots, p_r^Z, p_1^P, \dots, p_e^P)\} \rightarrow \{SK\left[Za_i\left(r_{j1}(x_1), \dots, r_{jm}(x_m)\right)\right] \rightarrow C[Za_i(y_{i1}, \dots, y_{ie})]\}.$

Етап 5. Досліджуються інформаційні особливості визначення оцінок параметрів у системі надання повноважень: $al_i[(x_{j1}, \dots, r_i^t(x_i), \dots, x_{jk})C_i(al_i)] \rightarrow SNP$

$\{\forall(Az_i \in SNP)\ \exists Az_j[Az_j(x_{i1}, \dots, r_i^t(x_i), \dots, x_{jk})] \rightarrow [C_i(Za_i) \approx C_i(al_i)]\} \rightarrow$

$\rightarrow \{[Az_i \rightarrow C_i(Za_i)] \rightarrow [C_i(Az_i \rightarrow Al_i(Za_i))]\}.$

Рисунок 1 – Метод формального опису даних

На *другому етапі* здійснюється аналіз суперечності між ціллю задачі та предметною областю, в якій використовуються результати її розв'язання.

Визначення 3. Аномалією An_i в W_i називаються наступні ситуації, що можуть виникати в W_i: виникнення структурної суперечності в W_i , виникнення логічної суперечності в W_i, виникнення семантичної суперечності в W_i.

Положення 2. Предметна область інтерпретації деякої системи є завжди зв'язною на структурному рівні.

Положення 3. Предметна область W_i не містить логічних суперечностей.

На *третьому етапі* здійснюється аналіз можливості розширення системи SNP та доводиться твердження про можливість розширення кількості рівнів конфіденційності в інформаційній системі.

Твердження 1. Якщо в IS існує система $R = \{r_1, \dots, r_m\}$ така, що $r_1 \prec r_2 \prec \dots \prec r_n$, то система R може бути розширена $r_{m+1} > r_m$.

На *четвертому етапі* здійснюється аналіз функціональних можливостей та оцінка окремих компонентів засобів захисту. Вводяться наступні визначення.

Визначення 4. Система доступу разом із засобами захисту доступу ($SD\&ZD$) розв'язує задачу визначення: чи користувач, що звернувся до IS, є санкціонований і ця задача розв'язується на основі аналізу даних, що характеризують самого користувача.

У відповідності з приведеним визначенням приймемо, що $SD\&ZD$ розв'язує задачу авторизації користувача, що можна описати наступним співвідношенням:

$$\left\{SD[k(p_1^k,\dots,p_r^k)]\&ZD(p_1^{SD},\dots,p_l^{SD}) \to Al^D\left(p_1^k,\dots,p_r^k,p_1^{/D},\dots,p_e^{lD}\right)\right\} \to$$
$$\to \{[(k \to sk)\&\neg(k \to NK)] \vee [(k \to NK)\&\neg(k \to sk)]\},$$

де p_i^k – параметр користувача; p_e^{lD} – параметр системи доступу; Al^D – алгоритм ідентифікації та авторизації користувача, що звернувся до IS із запитом за інформацією; k – користувач, статус якого є невизначеним в $SD\&ZD$.

Визначення 5. Система надання повноважень розв'язує проблему, що полягає у визначенні: чи задача, для розв'язання якої санкціонований користувач (SK) звернувся до системи, має повноваження на використання відповідних даних, тобто чи використання задачею Za_i даних $r_j(x_i)$ не призведе до недопустимих ситуацій в середовищі W_i, на яке орієнтована відповідна задача, що можна описати наступним співвідношенням:

$$\left\{\left[K(p_1^k,\dots,p_r^k)\&Za_i(p_1^z,\dots,p_g^z)\right] \to (SD\&ZD) \to Al^D(p_1^k,\dots,p_r^k,p_1^D,\dots,p_0^D)\right\} \to$$
$$\to \left\{Sk\left[Za(p_1^z,\dots,p_g^z)\right] \to (SNP) \to Al^{NP}(p_1^z,\dots,p_g^z,p_1^p,\dots,p_g^p)\right\} \to$$
$$\to \left\{Sk\left[Za[r_{j1}(x_1),\dots,r_{jm}(x_m)]\right] \to C[Za_i(y_{i1},\dots,y_{ie})]\right\},$$

де p_i^Z – параметри задачі; Al^{NP} – алгоритм визначення необхідних повноважень у задачі Za_i ; p_i^P – параметри системи SNP ; $r_{ji}(x_i)$ – дані x_i , що мають рівень конфіденційності r_{ji}; y_i – результат розв'язання задачі; C – мета розв'язання задачі Za_i. Для розв'язання сформульованої задачі забезпечення певного рівня безпеки системою $SB(IS)$, необхідно визначитися з параметрами задачі Za_i та з описом цілі C_i, розв'язання задачі $Za_i(y_{i1},\dots,y_{ie})$. Дані, які знаходяться в інформаційній системі, і особливо дані, що використовуються в прикладній задачі, не представляють собою деякі абстрактні величини. Вони завжди мають в рамках інформаційної системи і, відповідно, в рамках предметної області певну інтерпретацію, що записується у вигляді $j^s(x_i)$, якщо мова йде про інтерпретацію, що розміщується в інформаційній системі, та $j^W(x_i)$, якщо мова йде про інтерпретацію x_i в предметній області W_i. Прикладом інтерпретації x_i в інформаційній системі може служити інформація про допустимий діапазон значень даних x_i.

Визначення 6. Негативними факторами, що можуть виникати у W_i в результаті використання даних x_i з рівнем конфіденційності r_{ji} санкціонованим користувачем для розв'язання необґрунтованої задачі Za_i, є відповідні аномалії, що мають власну інтерпретацію.

У приведеному визначенні мова йде про санкціонованого користувача, яким є користувач, що пройшов ідентифікацію у системі. Це означає, що захищена інформаційна система доступу буде співпрацювати з користувачем. У рамках даного підходу довільний користувач звертається до інформаційної системи не просто за отриманням тих чи інших даних, а у випадку, коли ці дані мають певний рівень конфіденційності. Тому користувач повинен надати системі обґрунтування необхідності їх використання для розв'язання конкретної задачі.

На п'ятому етапі досліджуються інформаційні особливості визначення оцінок параметрів задач системою надання повноважень. При наданні повноважень SNP

розв'язується задача надання повноважень не користувачеві, який отримав статус SK, а надання повноважень задачі, що представляється SK і потребує тих чи інших даних, включаючи дані, що відносяться до категорії конфіденційних.

Метод визначення параметрів прикладних задач.

Визначення 7. Першому рівню конфіденційності даних $r_i^t(x_j)$, які використовуються при наданні повноважень задачі, відповідають дані $r_i^t(x_j)$, для перетворення яких в SNP існують визначені алгоритми $\{Az_j \dots Az_k\}$, що використовуються в процесі розв'язання задачі Za_i. Замість фрагменту алгоритм Al_i самої задачі, за умови, що Al_i має фрагмент, у якому сформовано необхідні умови для реалізації зазначеного фрагменту. Це означає, що Al_i орієнтований на використання даних типу $r_i^t(x_j)$ та описується ціль його реалізації. На основі цих даних SNP обирає адекватний $Az_i[r_i^t(x_j)]$ і передає результат перетворень до $Al_i(Za_i)$, що можна описати у вигляді:

$$al_i[(x_{j1}, \dots, r_i^t(x_i), \dots, x_{jk})C_i(al_i)] \rightarrow SNP\{\forall(Az_i \in SNP)\ \exists Az_j$$
$$[Az_j(x_{i1}, \dots, r_i^t(x_i), \dots, x_{jk})] \rightarrow [C_i(Za_i) \approx C_i(al_i)]\} \rightarrow$$
$$\rightarrow \{[Az_i \rightarrow C_i(Za_i)] \rightarrow [C_i(Az_i \rightarrow Al_i(Za_i))]\}.$$

Визначення 8. Другий рівень конфіденційності даних $r_i^{2t}(x_j)$, який використовується при наданні повноважень задачі, має місце у тому випадку, коли для досягнення цілі $C_i(al_i) \subset Al_i(za_i)$ в SNP не існує $Az_i(x_j)$, який забезпечував би досягнення цілі $C_i(Az_i) = C_i(al_i)$. На основі аналізу $C_i(al_i)$ та на основі аналізу інтерпретації $\{x_{j1}, \dots, x_{jk}\}$ обирається алгоритм директивного характеру Az_i^d, який формує результати обчислень, що зводяться до даних, які інтерпретуються на дискретній множині значень.

Визначення 9. Третій рівень конфіденційності $r_i^{3t}(x_j)$, який використовується при наданні повноважень задачі, має місце у тому випадку, коли на основі інтерпретаційних даних x_j та інтерпретації цілі $c(\mathrm{al}_i) \in Al_i(Za_i)$ приймаються рішення про неприпустимість безпосереднього використання x_j для розв'язання задачі Za_i, у зв'язку з чим система прийняття рішень (SPR), яка є складовою SNP, формує рекомендації щодо модифікації цілі $C(Za_i)$ в задачі Za_i з таким розрахунком, щоб можна було уникнути використання $r_i^{3t}(x_j)$.

У роботі доведено наступні твердження.

Eman 1. На основі приведених визначень будуємо формальний опис алгоритмів в є $\mathrm{Az_i}$ (алгоритми, що знаходяться в SNP) при визначенні повноважень задачі:
$al_i[(x_{j1}, \dots, r_i^t(x_i), \dots, x_{jk})C_i(al_i)] \rightarrow SNP\{\forall(Az_i \in SNP)\ \exists Az_j[Az_j(x_{i1}, \dots, r_i^t(x_i), \dots, x_{jk})] \rightarrow [C_i(Za_i) \approx C_i(al_i)]\} \rightarrow \{[Az_i \rightarrow C_i(Za_i)] \rightarrow [C_i(Az_i \rightarrow Al_i(Za_i))]\}$.

Eman 2. На основі приведених визначень обираються алгоритми A_i^d формування директив, які використовуються на другому рівні конфіденційності при визначенні повноважень задачі.

Eman 3. На основі інтерпретаційних даних x_j та інтерпретації мети $C_i(al_i) \in Al_i(Za_i)$ приймаються рішення про недопустимість безпосереднього використання x_j для розв'язання задачі Za_i. Тому система прийняття рішень (SPR), яка є складовою SNP, формує рекомендації щодо модифікації мети $C_i(Za_i)$ в задачі Za_i і для того, щоб можна було уникнути використання $r_i^{2t}(x_i)$.

Eman 4. Аналіз суперечності окремої задачі.

Eman 5. Аналіз повноти $\{SPR\&Az_i[r_i^{nt}(x_{i1}, \dots, x_{ik})]\}$ в SNP є повна відносно $Al_i(Za_i)$, де $Za_i \in W_i$.

Рисунок 2 – Метод визначення параметрів прикладних задач

Твердження 2. Якщо інформаційна система орієнтована на W_i, а задача Za_i обслуговує W_i з ціллю $C_i^t(Za_i)$, то в рамках засобів IS можна встановити наявність суперечності, яка може мати місце в $C_j\ (Za_i)$.

Твердження 3. Система $\{SPR\&Az_i[r_i^{nt}(x_{i1}, \dots, x_{ik})]\}$ в SNP є повна відносно $Al_i(Za_i)$, де $Za_i \in W_i$, а SPR система прийняття рішень з SNP.

У розділі запроваджено низку визначень, що стосуються рівнів конфіденційності, розроблено методи визначення параметрів інформаційних запитів прикладних задач і компонентів засобів захисту.

У третьому розділі досліджуються методи моделювання процесу функціонування динамічної системи надання доступу, а також основні компоненти моделі захисту системи доступу. Модель динамічної системи захисту доступу (MZD) включає в себе усі компоненти, що реалізують необхідні процеси. До таких процесів відносяться: ідентифікація користувачів – $h_i(ID)$; надання повноважень на використання даних задачі, яка звернулася за ними (SNP); управління рівнем конфіденційності даних – $r_i(x_i), (URT)$; управління рівнем значимості даних – $\aleph_i(x_i), (URZ)$; процеси оцінки рівня конфіденційності – $r_i(x_i)$ та параметрів інформаційних запитів задачі (OPS); процеси аналізу предметної області задач (APO); процеси визначення рівня безпеки інформаційної системи (ORB).

Метод визначення компонентів засобів захисту. Система надання повноважень на основі даних $Za[j(x_{i1}^z) * \dots * j(x_{ik}^z)]$, визначає: чи повноваження користувача K_i відповідають можливості доступу до даних, що уведені в задачу $Za[j(x_{i1}^z) * \dots * j(x_{ik}^z)]$; на основі аналізу $j(x_{ij})$, SNP визначає їх рівень конфіденційності, використовуючи дані $C_i[Za_i[j(y_{i1}) * \dots * j(y_{ik})]]$; система SNP встановлює відсутність суперечності в умові представленої задачі, оскільки IS, крім певних даних, має доступ до опису предметної області $W_i(IS_i)$, на обслуговування якої орієнтована IS.

Введемо наступні визначення, які доповнюють інформаційну систему.

Визначення 10. У рамках кожної IS_i визначаються критичні події, що можуть мати місце у відповідній області інтерпретації $W_i(IS_i)$, які будемо позначати символами $\mathcal{K}_i(W_i)$.

Визначення 11. Кожна критична подія призводить до виникнення в W_i критичної ситуації $\mathcal{K}_i(W_i)$.

Визначення 12. У предметній області W_i, на роботу з якою орієнтована система IS, критична ситуація виникає в результаті активізації відповідного процесу $Pr_i(\mathcal{K}r_i)$, який може виникнути у зв'язку з розв'язанням деякої задачі.

Визначення 13. Предметна область інтерпретації, що пов'язана з відповідною системою IS_i, має структуру $S(W_i)$, яка відображається на рівні логічних описів її фрагментів $g_i(\omega_i) \to L(\omega_i)$, а окремі фрагменти $\omega_i \in W_i$ складають графову структуру $G_i(W_i)$ предметної області W_i в цілому. Приведене визначення описується наступним формальним співвідношенням: $\{[g_{i1}(\omega_{i1}) \to L_{i1}(\omega_{i1})], \dots, [[g_{im}(\omega_{im}) \to L_{im}(\omega_{im})]\} \to GW_i$.

Доводиться твердження про неможливість виникнення суперечностей у процесах розв'язання задачі та визначення її актуальності.

Твердження 4. Розв'язання задачі Za_i, в якій мета $C_i(Za)$ не суперечить умовам W_i, не призведе до виникнення елементу $\omega_i{}^*$, що обумовить виникнення суперечності в $Pr_i(W_i^*)$, де $Pr_i(W_i^*) = Pr_i(W_i) * Pr_i(\omega_i^*)$.

Визначення 14. Актуальність задачі $Ak(Za_i)$ визначається рівнем прогресивності змін, які відбуваються в W_i в результаті використання отриманого розв'язання задачі.

Залежно від самої інформаційної системи, що орієнтована на обслуговування деякого середовища W_i, загальний параметр безпеки системи може складатися з цілого ряду окремих параметрів, що визначають загальний показник рівня безпеки β. До таких складових належать: параметр конфіденційності даних $(x_i^t(x_i))$; параметр важливості даних $\aleph_i(x_i)$; параметр актуальності задачі $Ak(Za_i)$; характеристика цілі задачі $C_i(Za_i)$; характеристика критичних ситуацій $\mathcal{K}_W(W_i)$; характеристика небезпек відносно інформаційної системи $Nb(IS)$. До параметрів інформаційного запиту задачі, які SNP перевіряє, для ідентифікації задачі, як окремого учасника, що співпрацює з IS, віднесемо наступні параметри: суперечність $C_i(Za_i)$ з початковими умовами $\sigma^i(C_i)$, актуальність задачі $Ak(Za)$, значимість задачі $\aleph_i(Za_i)$, рівень конфіденційності $r_i(Za_i)$.

Eman 1. Система SNP на основі даних $Za[j(x_{i1}^z) * ... * j(x_{ik}^z)]$ визначає наступну інформацію: чи повноваження користувача K_i відповідають доступу до даних, що потрібні для вирішення задачі $Za[j(x_{i1}^z) * ... * j(x_{ik}^z)]$.
Eman 2. На основі аналізу $j(x_{ij})$ SNP визначає рівень їх конфіденційності використовуючи дані $C_i[Za_i[j(y_{i1}) * ... * j(y_{ik})]]$, у зв'язку з цим система SNP визначає наявність або відсутність суперечності в умові представленої задачі
Eman 3. Система SNP на підставі даних про задачу Za_i отримує додаткову інформацію про Za_i з $W_i(IS_i)$
Eman 4. Аналіз критичних ситуацій
Eman 5. Аналіз логічності структури $\{[g_{i1}(\omega_{i1}) \to L_{i1}(\omega_{i1})], ..., [[g_{im}(\omega_{im}) \to L_{im}(\omega_{im})]\} \to GW_i$
Eman 6. Аналіз суперечностей
Eman 7. Аналіз актуальності
Eman 8. Аналіз значимості задачі
Eman 9. Обчислення рівня безпеки *IS*
Eman 10. Аналіз даних на базі рівня конфіденційності

Рисунок 3 – Метод визначення компонентів засобів захисту

Крім параметрів задачі, в рамках SNP реалізується перевірка даних, за якими задача звертається до IS. Система SNP ідентифікує відповідні параметри моделі даних на підставі реалізації аналізу параметрів, якими є: рівень конфіденційності $r_i(x_i)$; рівень значимості даних $\aleph_i(x_i)$; рівень обґрунтованості використання даних, який позначається $\lambda_i(x_i)$. Наведені параметри, що використовуються в SNP для надання повноважень Za_i на використання даних $\{x_i^z, ..., x_m^z\}$, можна розширити.

Крім параметрів інформаційних запитів задачі, система SNP перевіряє характер інформаційних особливостей даних, що існують в рамках задачі. Для використання цих параметрів у рамках моделі захисту доступу MZD, система SNP формує профілі задач, які будемо позначати $\psi(Za_i)$. Формально профіль $\psi(Za_i)$ запишемо у вигляді: $\psi(Za_i) = f[(P_1^I * P_2^I * ... * P_k^I), ..., (P_1^{Itk} * ... * P_k^{Itk}), \Delta t_i]$, де f – функція, яка описує спосіб визначення інтегрального значення параметру P_k^{Itk} за період Δt_i, I – параметр інформаційного типу. У більшості випадків функція f описує спосіб визначення середнього значення величини P_i^{Iti} на інтервалі Δt_i. До інформаційних особливостей P_i^I відносяться наступні: визначення, чи Za_i повинно поповнити IS новими даними з предметної області; аналіз, чи поточна задача Za_k не є повторенням задачі Za_i, яка уже розв'язувалася, що визначається на підставі співпадання мети цих задач; перевірка, чи поточна задача Za_i використовує ті ж самі вхідні дані, при різних цілях розв'язання задачі Za_i і однієї з попередніх задач Za_j.

Визначення 15. Параметри моделей даних, параметри інформаційних запитів задач та параметри перевірки інформаційних особливостей задач складають систему

параметрів, яка є повною для заданого рівня безпеки системи IS, що описується співвідношенням:

$$\beta(IS) = [r_i(x_i), \aleph_i(x_i), \lambda_i(x_i), \delta^S(Za_i), Ak(Za_i), \aleph_i(Za_i), r_j(Za_i), P_c, P_d, P_p].$$

Твердження 5. Система SNP забезпечує розпізнавання $r_i(x_i)$ за даними $j(x_i) \in Za_i$, якщо $j(x_i)$ збудовано відповідно до спільних для IS і W_i правил їх побудови.

Визначення 16. Система R представляє собою лінійну дискретну структуру з неоднорідними кроками дискретизації або $R = \{r_1^{1t}, r_2^{2t}, \dots, r_M^{mt}\}$, де верхній індекс означає номер рівня конфіденційності при заданому розподілі значень для кожного r_i.

Визначення 17. Обґрунтованість $\lambda_i(x_i)$ використання даних x_i в задачі Za_i визначається величиною різниці між цілями, одна з яких описує результат розв'язання задачі Za_i з використанням x_i, а друга – описує результат розв'язання тієї ж задачі без використання змінності x_i, що формально описується співвідношенням:

$$\lambda_i(x_i) = f\{C_i[Za_i](x_1, \dots, x_i, \dots, x_m)] * C_i[Za_i](x_1, \dots, x_{i-1}, \dots, x_{i+1}, .., x_i),$$

де f– функція, що описує спосіб обчислення різниці між цілями задачі Za_i.

У роботі запропоновано принцип побудови багаторівневої моделі системи доступу та проводиться її аналіз. Для цього вводяться наступні положення.

Положення 4. Необхідність введення параметру конфіденційності для x_i^* обумовлюється тим, що є можливим варіант використання цих даних, який може призвести до виникнення критичних ситуацій $\mathcal{K}r_i$ в середовищі використання результатів розв'язання задачі, яким є W_i.

Положення 5. Системи IS орієнтовано на обслуговування різних об'єктів, якщо вони потребують використання IS.

Твердження 6. Множина $\mathcal{K}r_i$ та, відповідно, множина An_i є обмеженими.

Твердження 7. Система $\{Az_i[r_i(x_i)], \dots, Az_m[r_m(x_m)]\}$ є повною відносно задачі Za_i.

Положення 6. Оскільки будь-які дані, у тому числі конфіденційні, мають свою предметну область визначення W_i, то параметри, що використовуються для їхнього опису, також повинні мати інтерпретацію в цій же предметній області.

Визначення 18. Довільна предметна область W_i, яка розглядається у даному випадку, представляє собою сукупність окремих об'єктів $\{y_i\}$, об'єднаних у певну структуру $S(X)$, яка може представлятися на графовому та логічному рівнях $G(Y)$ і $L(Y)$ відповідно, а також сукупність процесів $Pr_i(Y)$, які реалізуються у відповідних структурах, записується у вигляді: $W_i = \{G(Y), L(Y), Pr_i(Y)\}$.

Втрати, які можуть мати місце в W_i, обумовлюються виникненням аномалій $An_i(W_i)$ або виникненням критичних ситуацій $\mathcal{K}r_i(W_i)$.

Визначення 19. Кожна W_i функціонує відповідно до деякої стратегії або сукупності стратегій $St(W_i)$, які реалізуються на основі використання процесів Pr_i. $St(W_i) = F(Pr_i, \dots, Pr_m)$, де F – функція взаємозв'язків між Pr_i та Pr_m.

Визначення 20. Аномалією $An(W_i)$ є така зміна в середовищі W_i, що призводить до неможливості реалізації окремих процесів:

$$An(W_i) \to St(Pr_1, \dots, \neg Pr_i, \dots Pr_m).$$

Визначення 21. Критичною ситуацією $\mathcal{K}r_i(W_i)$ є така зміна в середовищі W_i, яка призводить до неможливості реалізації однієї із стратегій.

$$Kr_i(W_i) \to \{St_1 * \dots * \neg St_i * \dots * St_m\}.$$

Для використання приведених уявлень під час формування оцінки величини конфіденційності необхідно увести наступні умови та положення.

Умова 1. Діапазон вимірювання величини конфіденційності окремих даних буде представляти собою шкалу від нуля до 100, а одиницею вимірювання величини конфіденційності приймемо величину процентів.

Положення 7. Приймаємо, що можуть існувати алгоритми розв'язання задачі або відповідних задач Za_i, орієнтованих на досягнення мети, що полягає у впровадженні втрат в об'єкті або предметній області, де задача має інтерпретацію.

Положення 8. Можуть існувати задачі, орієнтовані на мету, що полягає у розвитку предметної області W_i та протидії можливим негативним факторам, дія яких на W_i у рамках предметної області має власну інтерпретацію.

Визначення 22. Рівень конфіденційності даних $r_i^t(x_i)$ визначається величиною втрат, до яких може призвести реалізація задачі, що використовує ці дані, метою якої є безпосередня або опосередкована дія на W_i, що призведе до втрат, величину яких можна визначити.

Положення 9. Кожне використання конфіденційної інформації призводить до пониження рівня її конфіденційності, як мінімум, за рахунок міграції інформації про ці дані в процесі, що реалізує розв'язання відповідної задачі.

У більшості випадків у середовищі W_i критичні ситуації призводять до негативних наслідків, коли вони активізуються тими чи іншими подіями. Серед таких подій можуть бути: події, що обумовлюються зовнішніми факторами, які не зв'язані безпосередньо з процесом $Pr_i[Za_i]$; події, що обумовлені процесом розв'язання окремої задачі, яка використовує конфіденційні дані та події, що обумовлюються самоактивізацією аномалій An_i чи $\mathcal{K}r_i$ в W_i.

У розділі запропоновано визначення, що стосуються взаємозалежності предметної області та параметрів, що характеризують задачі, описано принципи побудови багаторівневої системи.

У четвертому розділі досліджуються процеси надання повноважень та описується реалізація основних компонентів системи надання повноважень. У роботі досліджено та розроблено критерії прогресивності змін, до яких призводить використання результатів розв'язання задач, що використовують дані інформаційної системи.

Критерій 1. Якщо в результаті перетворень, які реалізуються алгоритмом $Al_i(Za_i)$ задачі Za_i, рівень конфіденційності вихідних даних є нижчим порівняно з рівнем конфіденційності вхідних даних, то відповідні перетворення і, відповідно Za_i, можна вважати актуальними.

Критерій 2. Якщо результатом розв'язання Za_i є нове правило перетворень, що передається в W_i, яке не призводить до суперечності в існуючій системі правил перетворень, то відповідну задачу Za_i можна вважати актуальною.

Критерій 3. Якщо в результаті передачі розв'язання задачі Za_i в систему W_i в останній елімінується аномалія, то така задача приймається прогресивною.

Критерій 4. Якщо в результаті розв'язання задачі Za_i, до W_i додається деяка компонента $\varphi_i(x_{is}, \dots, x_{ik})$, яка представляє певну структуру, що не є суперечною із структурами вхідних даних Dw_i та структурами предметної області W_i, то відповідна задача Za_i допускає інтерпретацію прогресивної задачі.

Оскільки в процесах аналізу параметрів інформаційних запитів задач і надання повноважень системою SNP використовуються інтерпретаційні описи даних, то в роботі вводяться наступні визначення.

Визначення 23. На рівні інтерпретації оберненість функціональних перетворень алгоритму $Al_i(Za_i)$ визначається на основі реалізації оберненої послідовності, що описується $j(Al_i) = j(al_{i1}) * j(al_{i2}) * ... * j(al_{im}), al_{ij} \in Al_i$.

Визначення 24. Інтерпретаційний опис x_i є повним для x_i, якщо будь-яке його розширення є надмірним.

Приведене визначення носить якісний характер, тому залежно від розширення інформації про оточення x_i величина і, відповідно, значення адекватності може збільшуватися.

Інформаційна система, як і кожний технічний об'єкт, характеризується надійністю, у визначенні якої основним акцентом є вимога щодо забезпечення виконання функціональних можливостей, які передбачено технічними умовами. Кінцевою метою роботи системи безпеки інформаційної системи також є забезпечення виконання нею функціональних можливостей. Для більш чіткого відокремлення обставин, що стосуються надійності та безпеки інформаційної системи, уведемо наступні умови.

Умова 2. Усі фактори штучного походження, що негативно впливають на процес функціонування інформаційної системи, приймаються як фактори, що загрожують безпеці системи.

Умова 3. Якщо система містить дані або інші елементи, використання яких може призвести до негативних наслідків в предметній області інтерпретації W_i, яку обслуговує система, то остання повинна включати засоби свого захисту.

Умова 4. Якщо на етапі проектування системи передбачається можливість виникнення негативних факторів невідомої природи, що характерно для систем, які функціонують порівняно довгий час, то в рамках системи передбачаються компоненти забезпечення можливості системи протидіяти таким факторам, тобто володіти здатністю розпізнавати невідомі негативні фактори та протидіяти їх впливу на систему.

Умова 5. Якщо в систему можна увести змінені дані, використання яких може призвести до наслідків, що не передбачалися функціональними вимогами до системи, то система повинна контролювати вхідні дані.

З наведених вище умов випливає, що під безпекою системи IS (на відміну від її надійності) вважається можливість системи безпеки протидіяти негативному впливу, який може виникнути при використанні результатів розв'язання задач. У роботі розроблено ряд алгоритмів, що реалізують результати досліджень.

На рис. 4 приведено блок-схему алгоритму, що відображає процес функціонування системи надання повноважень. Використовуються наступні умовні позначення: OD - перевірка, чи присутній текстовий опис даних; WD - визначення адреси даних; DT - визначення, чи дані є конфіденційними; VTZ - визначення рівня конфіденційності задачі; ZP - визначення, чи рівень конфіденційності задачі є більшим або дорівнює рівню конфіденційності даних; NSN - негативний вихід з системи надання повноважень; WPV - визначення параметра значимості моделі даних; ZD - перевірка, чи величина значимості моделі даних є допустимою; VPA - визначення параметра актуальності моделі даних; AD - перевірка, чи значення параметра актуальності моделі даних є допустимим; VPS - визначення рівня суперечності задачі; SZ - перевірка, чи величина суперечності задачі є допустимою; VAZ - визначення актуальності задачі; AZ - перевірка, чи величина актуальності задачі є допустимою; VZZ - визначення значимості задачі; ZZ - перевірка, чи величина значимості задачі є допустимою;

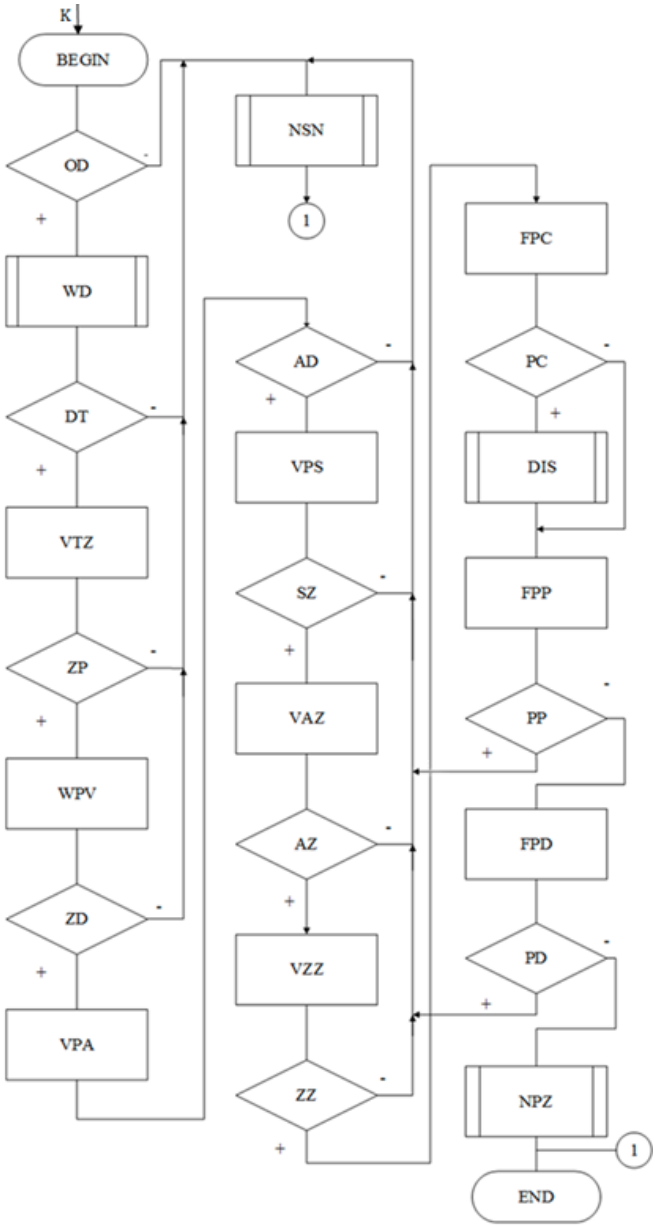

Рисунок – 4 Блок-схема процесу надання повноважень

FPC - формування параметру, що визначає можливість доповнення отриманими даними системи; PC - перевірка, чи повинна задача доповнити IS повними значеннями параметрів; FPP - формування параметру повторення задачі; DIS - доповнення інформаційної системи новими параметрами; PP - перевірка, чи задача не

повторюється; FPD - формування параметру дублювання задачі; PD - перевірка, чи має місце дублювання задачі; NPZ - надання повноважень задачі на використання даних, за якими задача звернулася до інформаційної системи.

На рис. 5 приведено блок-схему алгоритму, що відображає процес функціонування інформаційної системи.

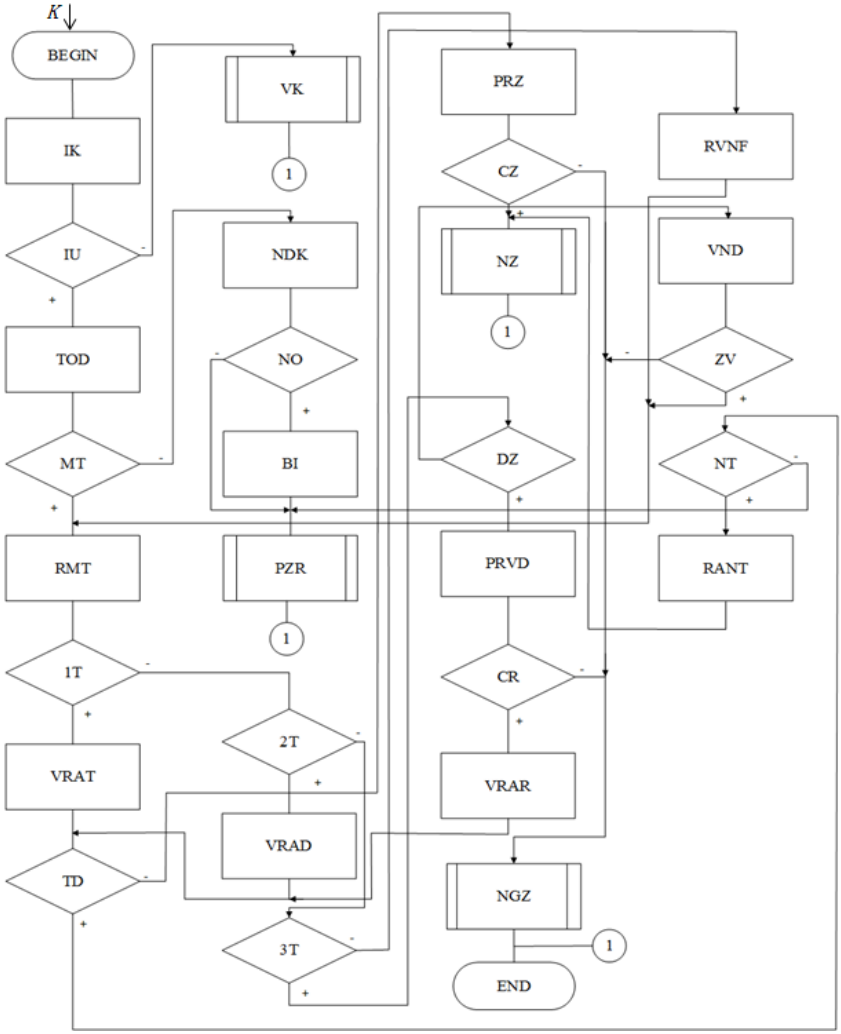

Рисунок – 5 Блок-схема загального функціонування інформаційної системи

$VRAT$ - вибір і реалізація відповідного внутрішнього алгоритму перетворення конфіденційних даних; TD - перевірка, чи є ще необхідність використання в задачі конфіденційних даних; CZ - перевірка, чи отримані результати відображають мету, яка описана в задачі; $2T$ - перевірка, чи дані відносяться до другого рівня конфіденційності; $VRAD$ - визначення і реалізація алгоритмів типу декларацій, що

використовують дані другого рівня конфіденційності; $ЗТ$ - визначення, чи дані відносяться до третього рівня конфіденційності; PRZ - прийняття рішень про дозвіл чи заборону використання даних третього рівня конфіденційності; DZ - перевірка, чи задача може використовувати дані третього рівня конфіденційності; $PRVD$ - прийняття рішення про спосіб використання конфіденційних даних третього рівня; CR - перевірка, чи мета задачі не суперечить можливому розв'язанню задачі; $VRAR$ - визначення і реалізація алгоритму, що відповідає прийнятому розв'язанню; $RVNF$ - реалізація відповідного фрагменту алгоритму задачі, що використовує неконфіденційні дані; NGZ - негативне завершення розв'язання задачі; VND - відмова у використанні даних третього рівня конфіденційності поточною задачею; ZV - перевірка, чи задача змінила вимоги до даних; NT - перевірка, чи використання конфіденційних даних є необхідне даній задачі; $RANT$ - реалізація фрагменту алгоритму, що не потребує конфіденційних даних; NZ - нормальне завершення роботи.

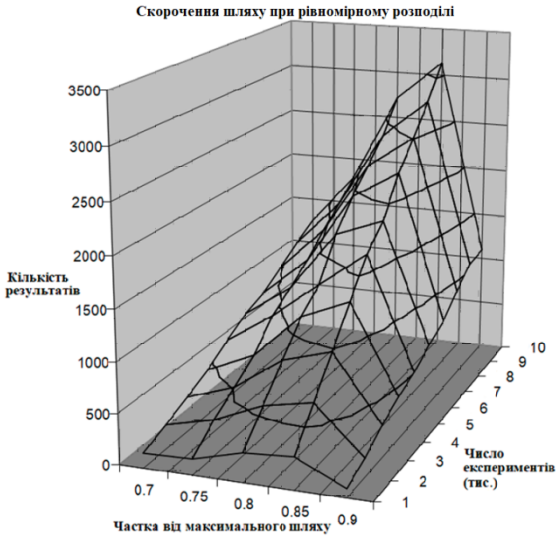

Рисунок 6 – Результати експериментальних досліджень

Проведені експериментальні дослідження підтвердили ефективність запропонованого розв'язання задач, а конкретний позитивний результат від практичного застосування запропонованої моделі залежить від прикладної задачі, що розв'язується.

Розглянемо варіант вирішення завдання щодо проведення об'єкта через закриту область, за наявності у ній динамічно переміщуваних об'єктів та за умови, що розголошення інформації про місце знаходження цих об'єктів неприпустимо. У стандартній моделі доступу об'єкт проводитися межею закритої області. А при використанні запропонованої дворівневої моделі доступу до даних з'являється можливість побудувати шлях через закриту область, при цьому приймається за критерій відсутність контакту між областю динамічного закритого об'єкта і його проводженням (рис. 6). Умови експерименту описано у дисертаційній роботі. За наявності чотирьох закритих об'єктів середній шлях при використанні дворівневої моделі доступу до даних становить 81%. Таким чином, позитивний результат від використання дворівневої моделі становить 19 відсотків.

У розділі приведено запропоновані визначення, сформульовано критерії та умови, що стосуються організації процесів функціонування системи надання повноважень та застосування дворівневої системи доступу, а також проведені експериментальні дослідження, які показали, що позитивний результат від використання дворівневої моделі становить 19 відсотків.

ВИСНОВКИ

У дисертаційній роботі розв'язано нову науково-прикладну задачу щодо підвищення рівня захисту конфіденційних даних в інформаційних системах на основі використання моделі багаторівневої системи надання повноважень на отримання конфіденційних даних, що дозволяє уникнути дії негативних факторів щодо впливу на систему надання повноважень, які виникають на нижчих рівнях доступу до функціонально орієнтованих інформаційних систем.

При цьому отримано наступні наукові результати.

1. Проведено аналіз методів захисту систем доступу користувача до функціонально орієнтованих інформаційних систем, який показав неможливість отримання частини інформації з консолідованого блоку більш високого рівня конфіденційності та відсутністю дробових способів доступу, що суттєво перешкоджає проведенню аналізу великих масивів даних за малою вибіркою.

2. Удосконалено методи формального опису параметрів інформаційних моделей даних, які зберігаються в інформаційній системі, та дозволяють визначати їх величини, що дало змогу проводити їх оцінку відповідно до необхідного рівня конфіденційності, завдяки чому розширилися можливості використання їх в прикладних задачах.

3. Уперше розроблено метод визначення параметрів інформаційних запитів користувачів та обчислення їх величин, а також використовуючи характеристики конфіденційних даних з інформаційної системи стало можливим, незалежно від користувача, надавати задачі повноваження на використання конфіденційних даних, у цьому випадку задача виступає як окремий суб'єкт, що дозволяє уникнути можливого впливу користувача на отримання цих даних.

4. Розроблено метод визначення параметрів додаткових компонентів засобів доступу до інформаційної системи, який дозволив порівняти рівень конфіденційності даних з величинами параметрів інформаційних запитів задач, завдяки чому стало можливим модифікувати повноваження доступу задачі, що звернулася із запитом до інформаційних ресурсів.

5. Уперше розроблено компоненти, що складають дворівневу модель доступу до даних, в якій компоненти відповідних рівнів функціонують незалежно, але переходи з нижчого рівня на вищий реалізуються на основі перевірок, що проводяться на відповідному рівні, що дозволяє збільшити рівень безпеки системи доступу і, як наслідок, виключити можливість виникнення негативного впливу на предметну область задачі, що розв'язується.

6. Розроблено моделі, практична реалізація яких забезпечила проведення поглибленого аналізу запропонованих методів, який підтвердив адекватність отриманих результатів, що також підтверджено даними за результати впровадження.

7. Розроблено алгоритми надання повноважень та загальної організації роботи дворівневої системи захисту доступу до даних, що забезпечує елімінацію суб'єктивних факторів користувача, які могли б впливати на можливість доступу до конфіденційних даних, а також проведені експериментальні дослідження, які показали, що позитивний результат від використання дворівневої моделі становить 19 відсотків.

ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Суліма О.А. Аналіз впливу параметрів даних на процеси надання повноважень / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – К. 2016. – С. 110-118.

2. Суліма О.А. Розробка алгоритму надання повноважень задачам на використання даних / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – К. 2016. – С. 110-116.

3. Давиденко А.М. Використання формальних засобів опису процесів надання повноважень / А.М. Давиденко, О.А. Суліма // Захист інформації. – К. 2016. Т. 18, – №2. – С. 143-149.

4. Суліма О.А. Аналіз основних систем надання повноважень користувачам. / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – К. 2017. – С. 66-74.

5. Суліма О.А. Аналіз методів оцінок рівня безпеки доступу до даних. / О.А. Суліма // Моделювання та інформаційні технології: Зб. наук. праць ІПМЕ НАН України. – К. 2017. – С. 35-42.

6. Суліма О.А. Модель багаторівневої системи доступу / О.А. Суліма // Безпека інформації. – К. 2017. – Т. 23. – С. 123-130.

7. Сулима О.А. Основные тенденции развития киберпреступности на рубеже 2015 года. /О.А. Сулима // Моделювання: XXXIV науково-технічна конференція. – К.: ІПМЕ ім. Г.Є. Пухова НАНУ, 2015. – С. 27.

8.Суліма О.А. Особливості використання засобів визначення повноважень в державних інформаційних системах / О.А. Суліма // Моделювання: XXXV науково-технічна конференція. – К.: ІПМЕ ім. Г.Є. Пухова НАНУ, 2016. – С.30

9. Суліма О.А. Аналіз процесів надання повноважень в інформаційно-телекомунікаційних системах / О.А. Суліма // Фундаментальні та прикладні дослідження у сучасній науці: IV наукова конференція. – Х.: Технологічний центр, 2016. – С. 67-68.

10. Суліма О.А. Побудова моделі доступу на базі моделі Діона. / О.А. Суліма // Міжнародна наукова конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" / Збірник тез доповідей: випуск 21, м. Тернопіль, 12 липня 2017 р., – Тернопіль. – 2017. – С. 55-57.

11. Суліма О.А. Визначення оцінок параметрів в системі надання повноважень / О.А. Суліма // Наукова конференція "Наука та інформація" . – К. Альманах – 2017. – С. 84-91.

АНОТАЦІЯ

Суліма О.А. Методи організації захисту доступу до інформаційних систем на основі використання багаторівневих моделей. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.21 - Системи захисту інформації. Національний авіаційний університет. Київ, 2017.

Дисертаційна робота спрямована на розроблення нових методів побудови системи надання повноважень для використання конфіденційних даних, що знаходяться в інформаційній системі. Система надання повноважень є важливою компонентою системи захисту доступу до інформаційної системи. У роботі досліджуються методи побудови систем надання повноважень, які забезпечують заданий рівень безпеки доступу до різних рівнів конфіденційних даних, що знаходяться в інформаційній системі.

У роботі розроблено та досліджено метод реалізації системи надання повноважень, який ґрунтується на використанні дворівневої моделі надання повноважень. Оскільки дані, що знаходяться в інформаційній системі, потрібні для розв'язання прикладних задач, то на першому рівні розглядається задача надання доступу до системи користувачу, який повинен розв'язати прикладну задачу. На

другому рівні система надає повноваження прикладній задачі, якій для розв'язання, крім інших даних, потрібні конфіденційні дані з певним рівнем конфіденційності. Задача надання повноважень прикладним задачам розв'язується на підставі аналізу параметрів задачі, і при цьому не приймаються до уваги параметри користувача. Очевидно, що необхідні параметри прикладної задачі представляє інформаційній системі користувач, який отримав доступ до системи.

Ключові слова: конфіденційність, повноваження, доступ, дані, параметри прикладної задачі, інформаційна система.

АННОТАЦИЯ

Сулима А.А. Методы организации защиты доступа к информационным системам на основании использования многоуровневых моделей. – Рукопись.

Диссертация на соискание научной степени кандидата технических наук по специальности 05.13.21 – Системы защиты информации. Национальный авиационный университет. Киев, 2017.

Диссертационная работа направлена на разработку новых методов построения системы предоставления полномочий для пользователей и задач с целью использования конфиденциальных данных, находящихся в информационной системе. Система предоставления полномочий является важным компонентом системы защиты доступа к информационной системе. Поэтому в работе исследуются методы построения систем предоставления полномочий, обеспечивающих заданный уровень безопасности доступа к разным уровням конфиденциальных данных, имеющихся в информационной системе.

В работе разработан и исследован метод реализации системы предоставления полномочий, основанный на использовании двухуровневой модели предоставления полномочий. Поскольку данные, находящиеся в информационной системе, нужны для решения прикладных задач, то на первом уровне рассматривается задача предоставления доступа к системе пользователя, который должен решить прикладную задачу. На втором уровне – система предоставляет полномочия прикладной задаче, которой для решения, кроме других открытых данных, нужны конфиденциальные с определённым уровнем конфиденциальности. Задача предоставления полномочий прикладным задачам решается на основе анализа ее параметров, при этом не принимаются во внимание параметры пользователя. Очевидно, что необходимые параметры прикладной задачи предоставляет системе пользователь, имеющий доступ к системе.

В первом разделе анализируются известные методы предоставления полномочий пользователям. Наиболее известный подход основывается на использовании матричных моделей, описывающих взаимосвязи между пользователями и объектами, к которым необходимо предоставить доступ и полномочия пользователю, на основании чего последний получает их по отношению к соответствующим объектам. Также анализируются известные методы оценки уровня безопасности системы, в первую очередь метод, который использует понятие риска.

В работе исследуются параметры, характеризующие данные, находящиеся в информационной системе, и используются в процессах предоставления полномочий для их использования. К таким данным относятся, кроме параметра конфиденциальности, параметры значимости и актуальности данных, а также ряд других параметров. Вводится и исследуется метод построения двухуровневой системы оценки степени конфиденциальности данных. Разработаны также методы реализации алгоритмов предоставления полномочий при обращении задачи к соответствующему уровню конфиденциальности.

В результате работы построена двухуровневая система предоставления полномочий и доступа к информационной системе в целом. На первом уровне доступа производится проверка полномочий пользователя на работу с соответствующей информационной системой в целом, что реализуется путем решения задачи идентификации и аутентификации. На втором уровне решается задача предоставления доступа прикладной задаче к конфиденциальным данным для их использования. В этом случае система предоставления полномочий осуществляет анализ параметров задачи: параметры значимости, актуальности, полномочий задачи и некоторые другие, которые она имеет.

В работе исследуются компоненты общей системы безопасности, основными компонентами которой являются системы предоставления полномочий пользователю и отдельно – полномочий прикладной задаче. В связи с этим в работе исследуются представления об аномалиях, которые могут возникать в рамках информационной системы, а также представления о критических ситуациях, возникающих в предметной области интерпретации данных, находящихся в информационной системе. Такие критические ситуации в предметной области интерпретации данных могут возникать при использовании результатов решения прикладных задач в этой области.

Ключевые слова: конфиденциальность, полномочия, доступ, данные, параметры прикладной задачи, информационная система.

ABSTRACT

Sulima O. Methods of access security organizing to information systems based on multilevel models. – Manuscript.

A Thesis for the Academic Degree of Candidate of Technical Sciences. Specialty 05.13.21 Information security systems. – National Aviation University. Kyiv, 2017.

The dissertation is devoted to the development of methods for building an empowerment system for the use of confidential data contained in the information system. The empowerment system is an important component of the information system access security system. Therefore, the paper examines the methods of building a system for granting authority that provides a certain level of security access to confidential data, which are closely related to the degree of confidentiality of relevant data contained in the information system.

The method of implementation of the empowerment system, based on the two-level model of empowerment, was developed and investigated in the work. Since the data contained in the information system is required to solve applied problems, the first level examines the task of granting access to the system to the user who has to solve an application task. At the second level, the system grants the authority to an applied problem, which needs to be solved and requires for that, apart from other data, confidential data with a certain level of confidentiality. The task of granting authority to applied problems is solved on the basis of analysis of task parameters and, at the same time, the user parameters are not taken into account. Obviously, the required parameters of the applied task are given to the information system by the user, who has gained the access to the system.

Keywords: confidentiality, powers, access, data, applied task parameters, information system.

Підписано до друку 27.10.17. Зам. №27-10(1)/17.
Формат 60х84/16. Обл. вид. арк. 1,47. Наклад 100 прим.
Друк «НВФ «Славутич-Дельфін».
пр-т Космонавта Комарова, 1.
Тел./факс: 406-74-41