УДК 004.056.53

Михайло СТРЕЛЬБІЦЬКИЙ,
кандидат технічних наук, доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

Дмитро МУЛ,
кандидат технічних наук, доцент,
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

Євгеній ПРОКОПЕНКО,
кандидат технічних наук, доцент
Національна академія Державної прикордонної служби України
імені Богдана Хмельницького, м. Хмельницький

МЕТОД УЗГОДЖЕННЯ СИСТЕМ РОЛЬОВОГО РОЗМЕЖУВАННЯ ДОСТУПУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ

У статті проведено дослідження умов спільного функціонування різних версій систем рольового розмежування доступу в інформаційно-телекомунікаційних системах на стадії їх модернізації. Показано, що модернізація інформаційно-телекомунікаційних систем вимагає постійного узгодження формального опису ролей з функціями посадових осіб прикордонних підрозділів. Аналіз спільного функціонування різних версій систем рольового розмежування доступу показав потребу в роз-

робленні методу їх узгодження. У статті розроблена математична та структурна модель методу. Обґрунтовані умови, при яких неможливе виникнення недозволеного в жодній версії інформаційно потоку.

Ключові слова: *система рольового розмежування доступу, інформаційно-телекомунікаційна система, модернізація.*

Постановка проблеми у загальному вигляді. Аналіз структури та діяльності Державної прикордонної служби як правоохоронного органу спеціального призначення показав чітку ієрархію підпорядкування органів і підрозділів прикордонного відомства разом з інформаційно-телекомунікаційними системами (ІТС), функціонал яких розподілений за рівнями управління [1; 2]. Посадові особи прикордонної служби виконують певні функціональні обов'язки в межах своєї посади, яка сприймається як певна роль, узагальнена сутність, що становить визначений перелік функцій і підпорядкованість працівника. Таким чином, реальні системи вимагають запровадження моделей розмежування доступу побудованих на сутностях ролі, яка має певну множину прав і повноважень. Разом із тим інтенсивний процес реорганізації організаційно-штатної структури та вдосконалення самих ІТС вимагає постійного узгодження функцій посадових осіб прикордонних підрозділів з формальним описом ролей діючих ІТС. Варто зазначити, що ІТС прикордонних підрозділів функціонують на загальному полі даних, яке розгорнуто у центральному сховищі даних. Вищенаведене вимагає вирішення проблеми узгодження різних версій систем рольового розмежування доступу, які функціонують на загальному полі даних гетерогенної інтегрованої інформаційно-телекомунікаційної системи "Гарт" прикордонного відомства.

Аналіз останніх досліджень і публікацій, в яких започатковано вирішення даної проблеми та на які опираються автори. Уперше такий підхід був розглянутий на межі 70–80-х років у дослідженнях процесів розмежування доступу корпорацією IBM та отримав назву рольового розмежування доступу. На початку 80-х років була представлена модель Лендвера-Макліна, що зустрічається в літературі також під назвою MMS-моделі (Military Message System), що поєднує дискреційний і мандатний принципи розмежування доступу з

використанням поняття та механізму ролей. Трохи пізніше з'явилися і формальні визначення рольових основ управління доступом (Role-Based Access Control – RBAC) [3; 4].

Системи, побудовані на моделі рольового розмежування доступу передбачають розмежування процесу функціонування системи та роботи користувача на сеанси, у кожному з яких, у свою чергу, виділяється два послідовних етапи: ідентифікація та автентифікація [5].

Рольові моделі поєднують мандатний підхід до організації доступу через певну агрегацію суб'єктів та об'єктів доступу і, тим самим, забезпечують жорсткість правил розмежування доступу і дискреційний підхід, що забезпечує гнучкість у налаштуванні системи розмежування доступу на конкретні функціонально-організаційні процеси предметної області. Дані особливості рольової політики дозволяють будувати системи розмежування доступу (СРД) з хорошою керованістю у складних системах з великою кількістю користувачів та об'єктів, і тому знаходять широке застосування в практичних системах [5].

Разом із тим системи розмежування доступу, які побудовані за рольовою моделлю, не передбачають оперування об'єктами, що є спільними з іншими системами. Виникнення такої ситуації можливо при модернізації інформаційно-телекомунікаційних систем у складі відомчих автоматизованих систем. На цій стадії апріорно різні версії програмного забезпечення оперують спільними даними. Для усунення колізій, викликаних відмінностями моделей розмежування доступу, необхідно здійснити завдання їх узгодження. Аналіз спільного функціонування різних версій систем рольового розмежування доступу показав наявність заборонених інформаційних потоків в обхід політики безпеки однієї із систем [6].

Мета статті. На підставі аналізу спільного функціонування рольових моделей розмежування доступу на загальному полі даних розробити метод їх узгодження, суть якого полягає у формуванні таких параметрів системи розмежування доступу, в якій неможливо реалізувати недозволений інформаційний потік у кожній з версій окремо.

Виклад основного матеріалу дослідження. Відповідно до формальної специфікації рольових моделей право доступу користувача

визначається призначеною роллю, яка в свою чергу містить певний набір повноважень (рис. 1).

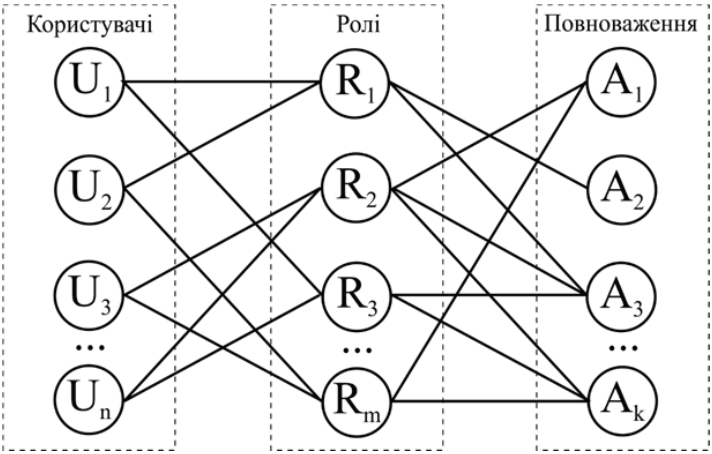

Рис. 1. Приклад надання користувачам ІТС певних повноважень через їх ролі

Так, через відображення множин сутностей рольової системи розмежування доступу можна визначити відображення множини користувачів на множину повноважень.

У роботі [3] наведені різновиди рольових моделей, залежно від можливих відносин між ролями, у тому числі передачі (делегування) повноважень і прав від одних ролей іншим ролям:

із ієрархічною організацією системи ролей;

взаємовиключними на будь-які сеанси ролями (модель статичного розподілу обов'язків);

взаємовиключними на один сеанс ролями (модель динамічного розподілу обов'язків);

кількісними обмеженнями за ролями;

групуванням ролей і повноважень.

Наведені різновиди моделей тільки формують види відображень множини користувачів на множину ролей і множину повноважень на множину ролей, кінцевим результатом яких є відображення множи-

ни повноважень на множину користувачів у конкретний момент часу функціонування системи. Вищезазначене дозволить сформувати математичну модель методу узгодження рольових СРД.

Інформаційно-телекомунікаційна система, в якій спільно функціонують дві різні версії рольових СРД (за необхідності узгодження більшої кількості метод може бути розширений за рахунок попарного узгодження) є сукупністю таких множин обох версій:

$U_1, U_2; U_1 \in U, U_2 \in U$ – множини користувачів;

$R_1, R_2; R_1 \in R, R_2 \in R$ – множини ролей;

$A_1, A_2; A_1 \in A, A_2 \in A$ – множини повноважень;

$F_1^{AR} : A_1 \mapsto R_1, F_2^{AR} : A_2 \mapsto R_2$ – відображення множини повноважень на множину ролей;

$F_1^{UR} : U_1 \mapsto R_1, F_2^{UR} : U_2 \mapsto R_2$ – відображення множини користувачів на множину ролей.

Зазначимо, що множини повноважень однозначно визначають операції над об'єктами та, відповідно, і самі об'єкти, над якими здійснюються визначені операції. Ця вимога накладає певні обмеження на множини повноважень, а саме повноваження різних версій СРД повинні бути атомарними на загальній множині повноважень A:

$$P_i \cap P_j = \varnothing, \forall P_i \in P, \forall P_j \in P. \quad (1)$$

Для випадку, коли $A_1 \setminus A_2 = \varnothing$ спільні повноваження різних версій СРД відсутні, а це в свою чергу унеможливлює виникнення будь-яких інформаційних потоків між користувачами з причини відсутності спільних об'єктів. В іншому випадку, коли $A_1 \setminus A_2 \neq \varnothing$ – множини повноважень різних версій СРД перетинаються, що може призвести до недозволених інформаційних потоків. Визначимо множину повноважень користувачів як:

$$U_i^A = \left\{ A_j, F^{U_i R} \cap F^{AjR} \neq \varnothing \right\}. \quad (2)$$

Дані множини є підґрунтям визначення можливості узгодження обох версій СРД, а саме у випадку виконання умови

$$\left(U^{A_1} \cap U^{A_2} = \varnothing\right) \cup \left(U^{A_1} \setminus U^{A_2} = \varnothing\right), \tag{3}$$

повноваження користувачів не суперечать один одному.

Отже, різні версії СРД можуть бути узгоджені. В іншому випадку, необхідно забезпечити дотримання основного правила безпеки для рольових СРД, а саме: система функціонує безпечно, якщо і тільки якщо будь-який користувач $u \in U$, який працює в сеансі $c \in C$ може здійснювати дії в межах повноваження $a \in A$, за умови, де $A \in f_{permission}(c)$ [3]. Це вимагає рівності повноважень для спільних для обох версій СРД користувачів, тобто:

$$U_i^{A_1} = U_i^{A_2}, \forall U_i^{A_1} \in U_R, \forall U_i^{A_2} \in U_R. \tag{4}$$

Вищезазначене дозволяє сформувати структурну модель методу узгодження різних версій рольових систем розмежування доступу (рис. 2).

У випадку невиконання умови (4) отримуємо множини користувачів, ролей і повноважень, які спричиняють порушення правила безпеки при спільному функціонуванні обох версій СРД і потребують зміни:

$$U_d = \{U_i\}, U_i^{A_1} \neq U_i^{A_2}, \forall U_i^{A_1} \in U_R, \forall U_i^{A_2} \in U_R, \tag{5}$$

$$R_d = F_1^{UR}(U_d) \cup F_2^{UR}(U_d), \tag{6}$$

$$A_d = \bar{F}_1^{AR}(R_d) \cup \bar{F}_2^{AR}(R_d), \tag{7}$$

де $\bar{F}$ – зворотне відображення множини ролей на множину повноважень

Перерозподіл ролей та (або) повноважень між різними версіями СРД здійснюється адміністраторами систем з урахування функціональних завдань користувачів. За потреби окремі повноваження користувачів можуть бути обмежені на період модернізації, після завершення якої відновлені.

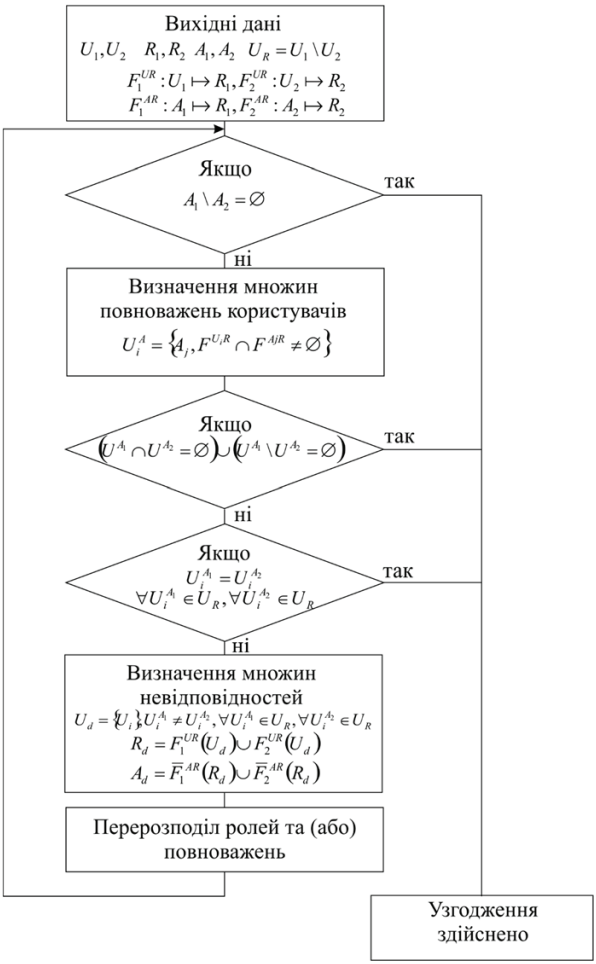

Рис. 2. Структурна модель методу узгодження різних версій рольових систем розмежування доступу

Висновки дослідження та перспективи подальших розвідок у даному напрямку. Отже, розроблений метод узгодження різних версій рольових систем розмежування доступу дозволить формально описати процедуру спільного функціонування обох інформаційно-телеко-

мунікаційних систем з питань безпеки інформації та визначити умови, за яких неможливе виникнення недозволених інформаційних потоків.

У подальшому, на підставі розроблених методів узгодження різних моделей розмежування доступу, пропонується розробка методологічного базису узгодження моделей розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації.

Список використаної літератури

1. Про Державну прикордонну службу України : Закон України / Відомості Верховної Ради України (ВВР). – 2003. – № 27. – Ст. 208.

2. Порядок функціонування, застосування та використання Інтранет-мережі Державної прикордонної служби України : наказ Адміністрації Державної прикордонної служби України від 09.08.2004 № 663.

3. Гайдамакин Н. А. Теоретические основы компьютерной безопасности : учеб. пособие / Н. А. Гайдамакин. –Екатеринбург, 2008. – 212 с.

4. Девянин П. М. Обзорные лекции по моделям безопасности компьютерных систем / П. М. Девянин // Прикладная дискретная математика : Институт криптографии, связи и информатики. – Москва. – 2009. – Вып. 2. – 152 с.

5. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. – Київ.

6. Стрельбіцький М. А. Аналіз спільного функціонування моделей розмежування доступу на стадії модернізації інформаційно-телекомунікаційних систем / М. А. Стрельбіцький // Збірник наукових праць Національної академії Державної прикордонної служби України імені Б. Хмельницького. Серія : військові та технічні науки. – №4 (70). – 2016 р.

Рецензент – доктор технічних наук, професор Андрощук О. С.

Стрельбицкий М., Мул Д., Прокопенко Е. **Метод согласования систем ролевого разграничения доступа информационно-телекоммуникационных систем на стадии модернизации**

В статье проведено исследование условий совместного функционирования различных версий систем ролевого разграничения до-

ступа в информационно-телекоммуникационных системах на стадии их модернизации. Показано, что модернизация информационно-телекоммуникационных систем требует постоянного согласования формального описания ролей с функциями должностных лиц пограничных подразделений. Анализ совместного функционирования различных версий систем ролевого разграничения доступа показал потребность в разработке метода их согласования. В статье разработана математическая и структурная модель метода. Обоснованы условия, при которых невозможно возникновение неразрешенного в каждой из версий информационного потока.

Ключевые слова: *система ролевого разграничения доступа, информационно-телекоммуникационная система, модернизация.*

Strelbitskii M.,Mul D., Prokopenko Y. **Role-based access control adjustment method of the information and telecommunication systems at the stage of modernization**

Permanent modernization and improvement process of a departmental information and telecommunication systems automation requires considering the possibility of joint operation of different versions of information security. The integration of new and old one means entails the transfer of the yearly functional tasks, algorithms of their solution and security mechanisms in the new software and hardware environment. The result is a common data field that is used by the old and new components of automated systems. At this stage of the system's life cycle the problem of transition to new software and hardware platform without disturbing the life cycle is arising.

The analysis of the access basic models has shown that one do not provide the other similar models joint operation on the general data field as one is possible in the information and telecommunication systems modernization.

Formation of the information and telecommunication systems' security policy, subject which ensured the information reliability is impossible without models of information security, as formalized description of its basic principles. Only through formal models one can prove the system's security by relying on the postulates of mathematical theory. The Security Models defines the basic principles of the security policy functions and used

in its construction, formation of technological solutions and justifying the system's ability to provide information reliability.

It is necessary to carry out the task of coordination of the automated systems under condition of their modernization when in the old and new versions of software are a priori implemented information security functions to resolve the conflicts caused by differences in the models.

The role-based access control system does not involve handling objects that are shared with other systems. This situation is possible during the modernization of information and telecommunication systems. Analysis of the joint functioning of different versions of role- based access control systems showed the presence of forbidden information flows bypassing the security policy of one of the systems. The mathematical and structural model of the method are developed in the article. The conditions under which it is impossible to cause the disable information flow in each version are justified.

The developed role-based access control adjustment method will allow formally describe the procedure for the joint operation of both information and telecommunication systems.

In the future, based on the developed access control adjustment methods it is proposed to develop a methodological basis for the joint of the models for the different of access to information and telecommunication systems at the stage of modernization.

Keywords: *role-based access control system, information and telecommunication system, modernization.*