УДК 004.056.53

Михайло Анатолійович Стрельбіцький *(канд. техн. наук, доцент)*

НаціональнаакадеміяДержавноїприкордонноїслужбиімені Б. Хмельницького, Хмельницький, Україна

МЕТОД УЗГОДЖЕННЯ МАТРИЦЬ ДОСТУПУ СИСТЕМ ДИСКРЕЦІЙНОГО РОЗМЕЖУВАННЯ ДОСТУПУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ НА СТАДІЇ МОДЕРНІЗАЦІЇ

В статті проведено аналіз умов при яких можливе виникнення недозволеного інформаційного потоку в одній із версій систем дискреційного розмежування доступу інформаційно-телекомунікаційних систем при спільному їх функціонуванні на стадії модернізації. Розроблено метод узгодження матриць доступу систем дискреційного розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації, який дозволить формально описати процедуру спільного функціонування обох систем розмежування доступу на загальному полі даних та визначити умови, при яких неможливе виникнення недозволених інформаційних потоків.

Ключові слова: *модель дискреційного розмежування доступу, інформаційно-телекомунікаційна система, модернізація*

Постановка проблеми

Виконання основних функцій Державної прикордонної служби України [1] з питань здійснення в установленому порядку прикордонного контролю і пропуску через державний кордон України осіб, транспортних засобів, вантажів, а також виявлення і припинення випадків незаконного їх переміщення, ведення інформаційно-аналітичної діяльності, координація діяльності військових формувань та відповідних правоохоронних органів, пов'язаної із захистом державного кордону України, а також діяльності державних органів, що здійснюють різні види контролю при перетинанні державного кордону України пов’язане із зберіганням та обміном інформації службового характеру між суб’єктами інтегрованого управління кордонами.

По мірі розвитку і розширення сфери застосування обчислювальної техніки все більша частина діяльності органів охорони державного кордону приходиться на автоматизовану обробку інформації. За допомогою програмно-апаратних засобів обчислювальної техніки виконуються операції над даними, від забезпечення безпеки яких залежить вирішення покладених на ДПСУ функціональних завдань. Разом із тим, постійна модернізаціяпрограмно-технічних комплексів автоматизації окремих завдань прикордонного відомства вимагає узгодження різних версій систем розмежування доступу, які функціонують на спільному полі даних.

Аналіз останніх досліджень і публікацій

Розробкою та дослідженням моделей дискреційного розмежування доступу присвячена значна кількість робіт дослідників. Перші роботи були опубліковані ще в 60-х роках минулого століття. Найбільш відомі з них: модель ADEPT-50 на замовлення МО США, п’ятивимірний простір Хартсона, модель Харрісона–Руззо–Ульманата інші. Зазначені моделі оперують дискретним набором трійок «суб’єкт–потік (операція)–об’єкт» .

Разом із тим, структура політик безпеки, які базуються на моделяхдискреційного розмежування доступу не передбачає оперування спільними з іншимисистемами об’єктами та суб’єктами, як це можливо при модернізації інформаційно-телекомунікаційних систем у складі відомчих автоматизованих систем.

Формулювання мети статті

На підставі аналізу спільного функціонування моделей дискреційного розмежування доступу розробити метод узгодження матриць доступу різних версій систем розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації.

Виклад основного матеріалу

Безпека інформації, що циркулює в інтегрованій інформаційно-телекомунікаційній системі (ІІТС)прикордонного відомства забезпечується коректним формуванням політики безпеки яка базується на відомих, формально доказаних моделях безпеки. Саме принципи на яких базуються моделі безпеки обґрунтовують здатність системи забезпечувати безпеку інформації.

На стадії модернізації ІІТС, тобто в умовах спільного функціонування різних версій систем розмежування доступу (СРД), можливе виникнення недозволеного інформаційного потоку. Тому, на цьому етапі життєвого циклу, коли апріорно різні версії програмного забезпечення оперують спільними даними, для усунення колізій, викликаних відмінностями моделей розмежування доступу, необхідно здійснити завдання їх узгодження.

Моделі дискреційного розмежування доступу (Харісона–Руззо–Ульмана, типізованих матриць доступу, Take–Grant, розширена модель Take–Grant та інші) оперують матрицею доступу $M\left[s_i, o_j\right]$, рядки якої відповідають суб'єктам $S = \{s_i\}$, стовбці об'єктам $O = \{o_j\}$ системи, а комірки визначають право доступу суб'єкта s_i на об'єкт o_j [2].

Розглянемо дві ситуації при яких можливе порушення політики безпеки в умовах функціонування на загальному полі даних різних версій СРД, які базуються на моделі дискреційного розмежування доступу.

Перша ситуація, значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів різні, тобто $\exists s_i, \exists o_j$ при яких $M_1\left[s_i, o_j\right] \neq M_2\left[s_i, o_j\right]$, де $s_i \in S_1, s_i \in S_2, o_j \in O_1, o_j \in O_2$. В даному випадку наочне порушення політики безпеки, так як при здійсненні операції суб'єкта у відношенні до об'єкта яку дозволяє СРД однієї версії є забороненою у іншій версії або навпаки.

У другому випадку значення прав доступу різних версій СРД для спільних суб'єктів та об'єктів однакові, тобто $M_1\left[s_i, o_j\right] = M_2\left[s_i, o_j\right]$, для $\forall s_i \in S_1, \forall s_i \in S_2, \forall o_j \in O_1, \forall o_j \in O_2$. Разом із тим, наявність суб'єктів та об'єктів які не входять до СРД іншої версії дозволяють здійснити інформаційний потік в обхід політики безпеки однієї із версій (рисунок 1).

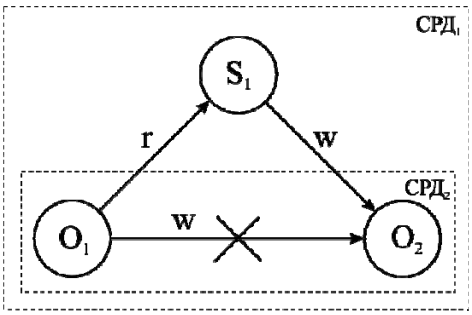

Рисунок 1 – Варіант реалізації інформаційного потоку в обхід політики безпеки однієї із версій системи розмежування доступу

На рисунку 1 показаний один елемент (суб'єкт S_1) який присутній в першій СРД та відсутній в другій і через який здійснюється інформаційний потік в обхід матриці доступу $M_2\left[s, o\right]$. Необхідно зазначити, що однією із властивостей інформаційних потоків є їх транзитивність, тому при визначенні «обхідного» інформаційного потоку необхідно враховувати всі об'єкти та суб'єкти системи.

Таким чином, дотримання безпеки інформації в умовах спільного функціонування різних версій СРД вимагає розробки методу їх узгодження.

Метод узгодження матриць доступу різних версій систем розмежування доступу призначений для формування спільної для обох версій СРД матриць доступу на етапі модернізації інформаційно-телекомунікаційних систем.

Суть методу узгодження матриць доступу різних версій систем розмежування доступу полягає у формуванні спільної для обох версій єдиної матриці доступу в якій неможливо реалізувати недозволений інформаційний потік в кожній з версій СРД окремо (рисунок 1).

Для аналітичного опису методу опишемо вихідні дані.

$M^{old}_{|S_{old}|\times|O_{old}|} = M^{old}\left[s_{old}, o_{old}\right]$ – матриця доступу старої версії СРД;

$M^{new}_{|S_{new}|\times|O_{new}|} = M^{new}\left[s_{new}, o_{new}\right]$ – матриця доступу нової версії СРД;

$M^{join}_{|S_{join}|\times|O_{join}|} = M^{join}\left[s_{join}, o_{join}\right]$ – матриця доступу спільної версії СРД.

При чому, $S_{join} = S_{old} \cup S_{new}$ та $O_{join} = O_{old} \cup O_{new}$.

Визначимо множини суб'єктів та об'єктів які є спільними для обох версій СДР, а саме $S_{sub} = S_{old} \cap S_{new}$ та $O_{sub} = O_{old} \cap O_{new}$.

При умові невідповідності елементів матриць доступу як старої так і нової версій СРД узгодження матриць є неможливим, тому спільне функціонування обох версій системи розмежування доступу приведе до порушення конфіденційності інформації. Таким чином, необхідною, але не достатньою умовою узгодження різних версій СРД, а саме їх матриць доступу, є:

$$M^{old}[s,o] = M^{new}[s,o], \forall s \in S_{sub}, \forall o \in O_{sub} \quad (1)$$

Наступним етапом методу є визначення можливості створення інформаційного потоку який є легальним в одній версії СРД та нелегальний в іншій.

Вихідними умовами узгодження різних версій СРД є те, що політика безпеки в кожній із них окремо сформована коректно та не допускає порушення надійності інформації. Тому необхідно розглядати тільки спільну частину матриць доступу різних версій СРД, а саме $M^{sub}_{|S_{sub}|\times|O_{sub}|} = M^{sub}\left[s_{sub}, o_{sub}\right]$ при дотриманні умови (1). Узгодженість різних версій СРД, а саме спільної матриці доступу $M^{join}\left[s_{join}, o_{join}\right]$ можлива тільки при рівності інформаційних потоків щодо об'єктів $M^{sub}_{|S_{sub}|\times|O_{sub}|}$ в різних матрицях доступу.

Нехай, $F^{old}_{|O_{sub}|\times|O_{sub}|} = \Re\left(M^{old}_{|S_{old}|\times|O_{old}|}, O_{sub}\right)$, $F^{new}_{|O_{sub}|\times|O_{sub}|} = \Re\left(M^{new}_{|S_{new}|\times|O_{new}|}, O_{sub}\right)$ – бінарні матриці інформаційних потоків старої та нової версій СРД між спільними об'єктами відповідно, а $\Re$ – оператор формування бінарної матриці інформаційних потоків між спільними об'єктами обох версій СРД та певної матриці доступу.

Вихідними даними для оператора формування бінарної матриці інформаційних потоків є матриця доступу $M_{|S|\times|O|} = M[s,o]$ та підмножина об'єктів O', де $O' \in O$.

Наступним етапом є формування матриці суміжності. З цією метою розіб'ємо множину прав доступу R на підмножини: $\vec{R} \in R$ – підмножина прав доступу яка формує інформаційний потік від суб'єкта до об'єкта (наприклад, право *write*), $\bar{R} \in R$ – підмножина прав доступу яка формує інформаційний потік від об'єкта до суб'єкта (наприклад, право*read*), $\tilde{R} \in R$ – підмножина прав доступу яка не формує інформаційний потік (наприклад, право *delete*). Елементи матриці суміжності $E_{|O|\times|O|} = \{e_{ij}\}$ формуються наступним чином:

$$e_{ij} = \begin{cases} 1, \exists k\, M[s_k, o_i] \in \bar{R}, M[s_k, o_j] \in \vec{R} \\ 0, else \end{cases} \quad (2)$$

В подальшому, враховуючи властивості графу [3] визначається матриця досяжності як кон'юнкція ступенів матриць суміжності, а саме:

$$E^* = \bigcup_{n=1}^{|O|} E^n \quad (3)$$

З метою зменшення розрахунків пропонується використати алгоритм (рисунок 2), суть якого полягає у припиненні розрахунків у випадку, якщо в наступній ітерації не з'являється новий шлях.

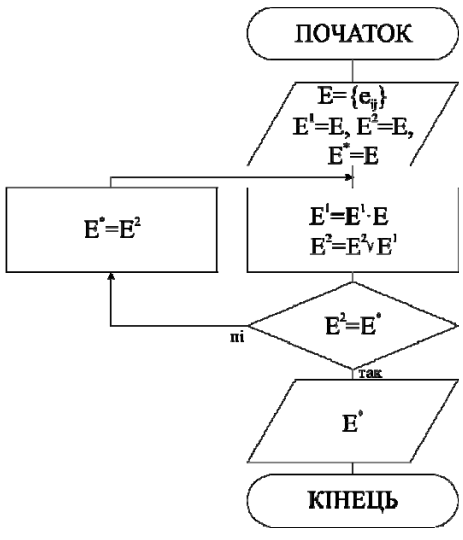

Рисунок 2 – Блок-схема алгоритму визначення матриці досяжності

Таким чином, результатом наведеної методики розрахунків є визначення бінарної матриці інформаційних потоків між спільними об'єктами обох версій СРД.

Використання вищезазначеного оператора дозволить сформувати множину інформаційних потоків враховуючи матриці доступу для кожної із версій СРД. Рівність бінарних матриць інформаційних потоків між спільними об'єктами в кожній версії свідчить про узгодженість обох версій СРД.

Структурна модель методу узгодження матриць доступу різних версій систем розмежування доступу представлена на рисунку 3.

Вищенаведений метод вимагає формулювання та доказу того, що при рівності інформаційних потоків спільних об'єктів обох версій СРД неможливо реалізувати заборонений інформаційний потік в однієї версії СРД та дозволений в іншій версії СРД (рисунок 1).

Теорема. Для узгодження різних версій СРД необхідно та достатньо забезпечити рівність інформаційних потоків між спільними об'єктами обох версій.

Доказ необхідності. В моделях дискреційного розмежування доступу недозволеним інформаційним потоком є потік який не передбачений матрицею доступу. Зазначимо, що окремо в кожній версії СРД матриця доступу сформована коректно та не допускає порушення конфіденційності інформації, тобто виникнення недозволеного інформаційного потоку. Таким чином, при рівності інформаційних потоків обох версій виникнення порушення безпеки інформації не можливе. Припустимо, що в одній із версій можливе виникнення недозволеного в іншій версії інформаційного потоку. Це означає що в одній версії СРД такий потік можливий, а в іншій ні, іншими словами передбачається наявність різних інформаційних потоків між суб'єктами та об'єктами СРД, що суперечить умові теореми.

Доказ достатності. Будь-яке порушення конфіденційності інформації передбачає наявність інформаційного потоку тільки до суб'єкта системи в супереч матриці доступу. Інформаційний потік між об'єктами не призводить до порушення конфіденційності. Разом із тим, передача інформації між суб'єктами можлива тільки через фізичний носій інформації (файл, база даних, тощо) – об'єкта системи. Таким чином, достатньо розглядати тільки спільні об'єкти системи, так як коректність інформаційних потоків не спільних об'єктів забезпечуються окремою версією СРД. Застосування методу узгодження матриць доступу різних версій систем дискреційного розмежування доступу здійснюється наступним чином. Перед спільним функціонуванням існуючої та модернізованої СРД здійснюється перевірка про можливість узгодження матриць доступу (виконання умови 1).

У випадку неможливості їх узгодження провадиться зміна параметрів доступу в одній із версій СРД з метою підготовки до наступного етапу методу. Далі здійснюється перевірка узгодженості інформаційних потоків різних версій СРД. У випадку виявлення невідповідності можлива корекція однієї із версій матриць доступу та повторна перевірка. При рівності інформаційних потоків для спільних об'єктів різні версії СРД можуть спільно функціонувати на загальному полі даних. При виникненні потреби динамічної зміни параметрів матриць доступу можливо реалізувати механізм узгодження, який здійснюватиме перевірку змін на наявність недозволених інформаційних потоків. Таким чином, при спільному функціонуванні існуючої та модернізованої ІТС неможливе виникнення недозволених інформаційних потоків і, як наслідок, порушення безпеки інформації.

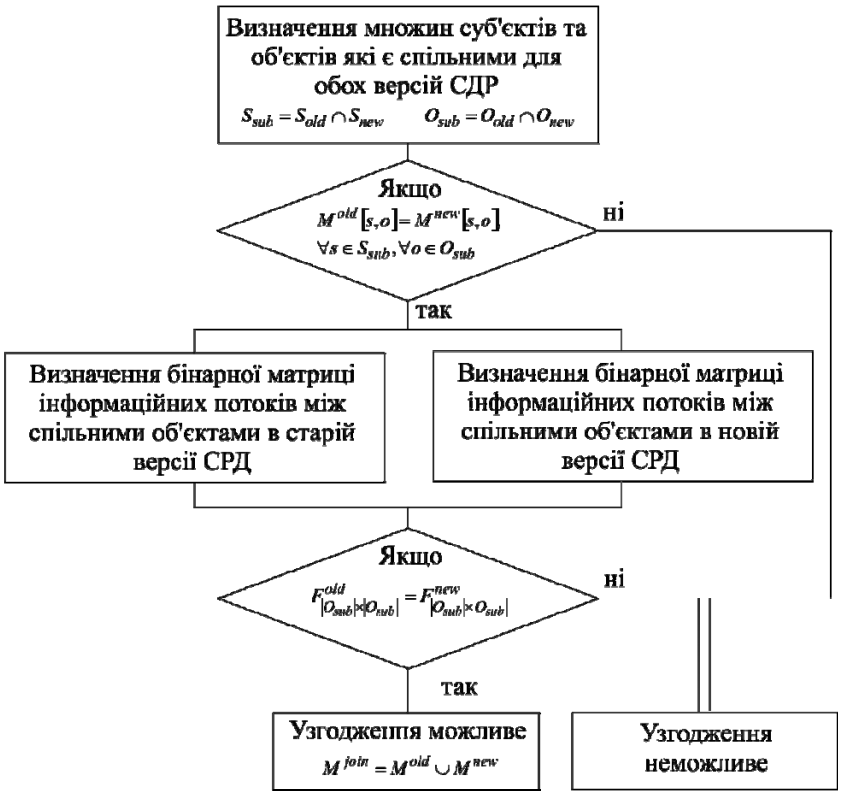

Рисунок 3 – Структурна модель методу узгодження матриць доступу різних версій систем розмежування доступу

Висновки

Розроблений метод узгодження матриць доступу різних версій систем дискреційного розмежування доступу дозволить формально описати процедуру спільного функціонування обох інформаційно-телекомунікаційних систем з питань безпеки інформації та визначити умови, при яких неможливе виникнення недозволених інформаційних потоків. Таким чином, запропонований метод є одним із базових в технології захисту інформації в інтегрованій інформаційно-телекомунікаційній системі Державної прикордонної служби України на стадії модернізації. Подальшим напрямком дослідження може бути розробка методів узгодження із системами розмежування доступу побудованих за іншими моделями.

Література

1. Закон України "Про Державну прикордонну службу України" Відомості Верховної Ради України (ВВР), 2003. **2. Девянин П.Н.** Моделибезопасностикомпьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр «Академия», 2005. – 144 с. **3. Домнин Л.Н.**Элементытеориграфов: учеб.пособие. – Пенза: Изд-во Пенз. гос. ун-та, 2007. – 144 с.

МЕТОД СОГЛАСОВАНИЯ МАТРИЦ ДОСТУПА СИСТЕМ ДИСКРЕЦИОННОГО РАЗГРАНИЧЕНИЯ ДОСТУПА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ НА СТАДИИ МОДЕРНИЗАЦИИ

***Михаил Анатольевич Стрельбицкий** (канд. техн. наук, доцент)*

Национальная академия Государственной пограничной службы Украины имени Б. Хмельницкого, Хмельницкий, Украина

В статье проведен анализ условий при которых возможно возникновение неразрешенного информационного потока в одной из версий систем дискреционного разграничения доступа информационно-телекоммуникационных систем при совместном их функционировании на стадии модернизации. Разработан метод согласования матриц доступа систем дискреционного разграничения доступа информационно-телекоммуникационных систем на стадии модернизации, который позволит формально описать процедуру совместного функционирования обеих систем разграничения доступа на общем поле данных и определить условия, при которых невозможно возникновение неразрешенных информационных потоков.

Ключевые слова: *модель дискреционногоразграничения доступа, информационно-телекоммуникационная система, модернизация*

METHOD OF THE RECONCILIATION OF THE ACCESS MATRICES OF THE DISCRETIONARY ACCESS CONTROL SYSTEMS OF THE INFORMATION AND TELECOMMUNICATION SYSTEMS AT THE STAGE MODERNIZATION

MykhajloAnatolijovychStreljbicjkyj (Candidate of Technical Sciences, Associate Professor)

The article analyzes the conditions under which may cause unauthorized information flow in one of the versions of discretionary access control of the information and telecommunication systems while their joint operation at the stage of modernization. The method of harmonization of the matrices of discretionary access control of the information and telecommunication systems at the stage of modernization is developed, which will formally describe the procedure for joint operation of the two systems of access to common data field and determine the conditions under which cannot be origin the unauthorized information flows.

Keywords: *model discretionary access control, information and telecommunication system, modernization.*

References

1. Lawof Ukraine "On the State Border Service of Ukraine" [Pro Derzhavnu prykordonnu sluzhbu Ukrajiny] Supreme Council of Ukraine (VVR), 2003. **2. Devyanin P.N.** Models of the security of computer systems [Modeli bezopasnosti kompyuternyih sistem]: Proc. allowance for students. Executive. Proc. institutions. - M .: Publishing Center "Academy", 2005. - 144 p. **3. Domnin L.N.** Elements of graph theory [Elementyiteoriigrafov]: Textbook. allowance. - Penza: IzdPenz. state. University Press, 2007. - 144 p.