УДК 004.056.53

д.т.н. Кузавков В.В. (ВІТІ)
к.т.н. Стрельбіцький М.А. (НАДПСУ)
Данько В.О. (ВІТІ)

МЕТОД УЗГОДЖЕННЯ РЕШІТОК РІВНІВ КОНФІДЕНЦІЙНОСТІ СИСТЕМ МАНДАТНОГО 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 мандатного розмежування доступу при спільному їх функціонуванні. Розроблено метод узгодження решіток рівнів конфіденційності систем мандатного розмежування доступу, який дозволить формально описати процедуру спільного функціонування обох систем на загальному полі даних та визначити умови, при яких неможливе виникнення недозволених інформаційних потоків.

Кузавков В.В., Стрельбицкий М.А., Данько В.О. Метод согласования решеток уровней конфиденциальности систем мандатного разграничения доступа информационно-телекоммуникационных систем на стадии модернизации. *В статье проведен анализ условий при которых возможно возникновение неразрешенного информационного потока в одной из версий систем мандатного разграничения доступа при совместном их функционировании. Разработан метод согласования решеток уровней конфиденциальности систем мандатного разграничения доступа, который позволит формально описать процедуру совместного функционирования обеих систем на общем поле данных и определить условия, при которых невозможно возникновение неразрешенных информационных потоков.*

V. Kuzavkov, M. Strelbitskiy, V. Danko Method of the reconciliation of the privacy grids of the mandate access control systems of the information and telecommunication systems at the stage modernization. *The article analyzes the conditions under which may cause unauthorized information flow in one of the versions of mandate access control systems while their joint operation. The method of harmonization of the grids of levels of confidentiality of access credentials systems is developed that will formally describe the procedure for joint operation of both systems at the general data field and determine the conditions under which cannot be origin the unauthorized information flows.*

Ключові слова: *решітка рівнів конфіденційності, модель мандатного розмежування доступу, модернізація.*

Постановка проблеми

Функціонування інформаційно-телекомунікаційних систем Державної прикордонної служби як суб'єкта забезпечення національної безпеки України [1] безпосередньо пов'язано із запобіганням основних загроз національним інтересам і національній безпеці України в інформаційній сфері. Широкомасштабна інтеграція програмно-технічних засобів автоматизації у практично у всі сфери діяльності прикордонного відомства вимагає постійного вдосконалення та модернізації складових інтегрованої інформаційно-телекомунікаційної системи (ІІТС). На теперішній час ІІТС складається більш як з 20 інформаційно-телекомунікаційних (ІТС) та інформаційних систем (ІС) та 10 підсистем, що забезпечують виконання різних функціональних завдань, систем забезпечення та взаємодії з іншими відомствами з питань національної безпеки України в прикордонній сфері. Особливістю ІІТС „Гарт" є функціонування її складових (ІТС, ІС, підсистем) на загальному полі даних, що дозволяє максимально ефективно аналізувати прикордонну інформацію. Ступінь безпеки інформації в інформаційно телекомунікаційних системах Державної прикордонної служби, як суб'єкта забезпечення національної безпеки, впливає на якість виконання завдань прикордонного відомства та, відповідно, на рівень національної безпеки України.

Разом із тим, виклики та загрози національній безпеці держави у прикордонній сфері вимагають постійної адаптації засобів автоматизації до вимог сьогодення. Це вимагає узгодження засобів захисту інформації при модернізації складових ІІТС (впровадження нових систем) які функціонують на загальному полі даних.

Аналіз останніх досліджень і публікацій

Розробкою та дослідженням моделей мандатного розмежування доступу (МРД) присвячена значна кількість робіт дослідників, серед яких Leonard J. LaPadula [2 – 3], D. Elliot Bell, Герасименко В.А., Грушо А.А. та інші [4 – 11]. При чому, на теперішній час

також розроблена та впроваджена в дію велика сукупність міжнародних та вітчизняних стандартів та нормативних документів у галузі інформаційної безпеки.

Разом із тим, структура моделей мандатного розмежування доступу не передбачає спільне функціонування з іншими моделями на загальному полі даних, як це можливо при модернізації інформаційно-телекомунікаційних системи у складі ІТС. Практично всі моделі присвячені розгляду статичної системи захисту, яка функціонує автономно та повинна забезпечувати захист інформації.

Мета статті. На підставі аналізу спільного функціонування моделей мандатного розмежування доступу розробити метод узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу інформаційно-телекомунікаційних систем на стадії модернізації.

Основний матеріал

Моделі інформаційної безпеки є базисом формування політик безпеки різних інформаційно-телекомунікаційних систем. Формальні моделі дозволяють довести безпеку системи відомими та апробованими методами наукових досліджень. Таким чином, політика безпеки ІТС, яка побудована за постулатами певної моделі інформаційної безпеки здатна гарантовано виконати функції щодо захисту інформації.

При розробці складових ІІТС формалізується та реалізовується певна політика безпеки, яка базується на відомих моделях інформаційної безпеки. Їх використання в окремих ІТС, ІС та підсистемах забезпечує виконання функцій захисту інформації. Разом із тим, при модернізації існуючих складових ІІТС або інтеграції нових виникає ситуація спільного функціонування систем захисту інформації на загальному полі даних.

Моделі мандатного розмежування доступу (класична модель Белла–ЛаПадули, модель безпечного переходу, модель систем воєнних повідомлень, політика low–watermark, модель цілісності Біба та інші) аналізують умови, при виконанні яких неможливий інформаційний потік від об’єктів з більшим рівнем конфіденційності до об’єктів з меншим рівнем конфіденційності [12]. В даних моделях кожний суб’єкт і об’єкт системи асоціюється з відповідним рівнем безпеки (конфіденційності).

Формалізуємо мандатну модель розмежування доступу як сукупність множин: об'єктів $\{O\}$, суб’єктів $\{S\}$ та дозволених моделлю операцій (інформаційних потоків) $\{\Omega\}$.

Якщо система МРД в складі старої версії представити у вигляді $\{S_1, O_1, \Omega_1\}$, а нової версії як $\{S_2, O_2, \Omega_2\}$, то для випадку, коли істинний, такий вираз:

$$\begin{aligned}&(S_1 \cap S_2 = \varnothing) \cap (O_1 \cap O_2 = \varnothing) \cap (\Omega_1 \cap \Omega_2 = \varnothing) \cup \\ &\cup (S_1 \setminus S_2 = \varnothing) \cap (O_1 \setminus O_2 = \varnothing) \cap (\Omega_1 \setminus \Omega_2 = \varnothing)\end{aligned} \quad (1)$$

колізії між новою і старою версіями СЗІ в ІІТС відсутні. Дана вироджена ситуація не входить в область дослідження.

Досліджувані суперечності мають місце, якщо результатом взяття декартової різниці між $S_1 \times O_1 \times \Omega_1$ та $S_2 \times O_2 \times \Omega_2$ буде відмінна від $\varnothing$ підмножина $S_R \times O_R \times \Omega_R$, яка, в загальному випадку, буде складатися з компонентів обох поколінь системи розмежування доступу (СРД).

Таким чином, при спільному використанні обома версіями системи МРД об’єктів та суб’єктів загального поля даних можливе виникнення недозволеного інформаційного потоку в одній із версій з причини невідповідності решіток рівнів конфіденційності об’єктів (рис. 1);

Вищезазначене вимагає розробки методу узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу.

Метод узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу призначений для формування спільної для обох версій СРД решітки рівнів конфіденційності на стадії модернізації інформаційно-телекомунікаційних систем.

Суть методу узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу полягає у формуванні спільної для обох версій єдиної решітки рівнів конфіденційності в якій неможливо реалізувати недозволений інформаційний потік в кожній з версій СРД окремо (рис. 1).

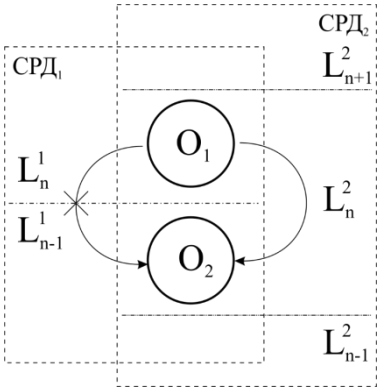

Рис. 1 – Реалізація інформаційного потоку в обхід політики безпеки однієї із версій системи розмежування доступу при невідповідності решіток рівнів конфіденційності

де L^1, L^2 – решітки рівнів конфіденційності старої та нової версій системи МРД.

Структурна модель методу узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу представлена на рисунку 2.

Рис. 2 – Структурна модель методу узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу

Визначення спільної для обох версій СРД функції перетворення меж решітки конфіденційності здійснюється в кожному випадку окремо. Прикладами такої функції може бути вартість втрати інформації, можливий збиток від порушення конфіденційності, тощо. На теперішній час розроблено достатньо представницький арсенал моделей оцінки інформації. В роботі [13] наведено окремі з них, а саме:

адитивна модель, в якій інформація представлена як кінцева множина елементів, де експерти здійснюють оцінку кожного елементу окремо, а вартість інформації представляється сумою вартостей її елементів;

аналіз ризику – модель, яка базується на адитивній моделі, але оцінюється вартість втрат, виходячи із прогнозу можливих загроз компонентам інформації;

порядкова шкала цінностей – модель, яка оцінює інформацію не за її грошовою оцінкою, а як порівняння цінностей окремих інформаційних елементів між собою;

модель решітки цінностей – узагальнена модель порядкової шкали цінностей.

Призначення зазначеної функція полягає у перетворенні формально описаних меж решітки конфіденційності в числові значення. Аналітично метод узгодження решіток рівнів конфіденційності різних версій систем розмежування доступу представляється наступним чином.

Нехай:

$(L^{old},\leq),(L^{new},\leq)$ та $(L^{join},\leq)$ – решітки рівнів конфіденційності старої, нової та спільної систем мандатного розмежування доступу;

$f(L)$ – функція перетворення меж решітки конфіденційності;

Тоді спільна для обох версій СРД решітка конфіденційності є:

$$(L^{join},\leq) = f^{-1}\left(f(L^{old},\leq) \cup f(L^{new},\leq)\right) \qquad (2)$$

де $f^{-1}(L)$ – обернена функція перетворення меж решітки конфіденційності;

Вищенаведений метод вимагає формулювання та доказу того, що у запропонованій спільній решітці конфіденційності неможливо реалізувати заборонений інформаційний потік в однієї версії СРД та дозволений в іншій версії СРД (рис. 1).

Теорема безпеки спільної решітки конфіденційності. У спільній решітці конфіденційності неможливо реалізувати заборонений інформаційний потік в однієї версії СРД та дозволений в іншій версії СРД.

Доказ. В системах розмежування доступу при використанні решіток конфіденційності недозволеним інформаційним потоком є потік від об'єктів з вищим рівнем конфіденційності до об'єктів з нижчим рівнем конфіденційності. Припустимо, що в спільній решітці конфіденційності можливий такий потік, який в одній із версій СРД дозволений, а в іншій заборонений. Це означає, що об'єкти повинні знаходитись в одній множині решітки конфіденційності однієї версії (дозволений інформаційний потік) та в різних множинах решітки конфіденційності іншої версії (недозволений інформаційний потік). Разом із тим, розбиття спільної решітки конфіденційності передбачає знаходження таких об'єктів в різних множинах спільної решітки конфіденційності (рисунок 3). Таким чином, зазначений інформаційний потік буде забороненим, що суперечить припущенню про його існування.

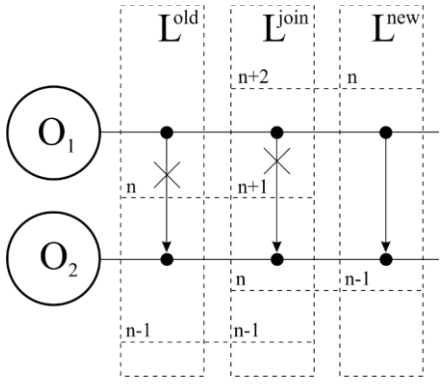

Рис. 3. До доказу теореми безпеки спільної решітки конфіденційності

Застосування методу узгодження решіток рівнів конфіденційності різних версій систем мандатного розмежування доступу здійснюється наступним чином. Перед спільним функціонуванням існуючої та модернізованої системи розмежування доступу здійснюється узгодження решіток рівнів конфіденційності та визначається спільна для обох версій решітка рівнів конфіденційності. Наступним етапом є зміна параметрів кожної із версій СРД у відповідності до сформованої спільної решітки рівнів конфіденційності. Заключним етапом є інтеграція модернізованої складової ІТС до загальної системи, при чому параметри СРД яких

вже узгоджені. Таким чином, при спільному функціонуванні існуючої та модернізованої ІТС неможливе виникнення недозволених інформаційних потоків і, як наслідок, порушення безпеки інформації.

Висновки дослідження перспективи подальших розвідок у даному напрямку. Розроблений метод узгодження решіток рівнів конфіденційності різних версій систем мандатного 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 основи національної безпеки України” Відомості Верховної Ради України (ВВР), 2003.

2. LaPadula L., Bell D. Secure Computer System: Mathematical Foundation, ESD-TR-73-278, V.1, MITRE Corportaion.

3. LaPadula L., Bell D. Secure Computer System: A Mathematical Foundation, ESD-TR-73-278, V.II, MITRE Corportaion.

4. Теория и практика обеспечения инфармационной безопасности / Под ред. П.Д. Зегжди. – М.: Издательство Агентства „Яхтсмен”, 1996.

5. Баранов А.П., Борисенко Н.П., Зегжда П.Д., Корт С.С., Ростовцев А.Г. Математические основи информационной безопасности. – Орел, 1997.

6. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Издательство Агентства „Яхтсмен”, 1996.

7. Kaliski Jr. B. S. A pseudo-random bit generator based on elliptic logarithms / B. S. Kaliski Jr. // Advances in Cryptology: Proceedings of Crypto '86 (Lecture Notes in Computer Science, vol. 263), Springer-Verlag, New York, 1987, pp. 84 – 103.

8. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, and M. Luby // Proceedings of the 21st Annual ACM Symposium on Theory of Computing, ACM, New York, 1989, pp. 12 – 24.

9. Burton S. One-Way Permutations on Elliptic Curves / Burton S., Kaliski Jr. // Journal of Cryptology (1991) International Association for Cryptologic Research. 1991. – P.187 – 199.

10. Thurimella R. Cryptography for Cyber Security and Defense: Information Encryption and Cyphering / R. Thurimella and L.C. Baird III // IGI Global, 2009, chapter title: „Network Security”.

11. Hoeper K. Monitoring-Based Key Revocation Schemes for Mobile Ad Hoc Networks: Design and Security Analysis / Katrin Hoeper, Guang Gong // Security and Privacy for Emerging Areas in Communication Networks. Waterloo, ON, N2L 3G1, Canada, 2009.

12. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. – М.: Издательский центр „Академия”, 2005. – 144 с.

13. Грушо А. А., Тимонина Е. Е. Ценность информации. – М.: Издательство Агентства „Яхтсмен”, 1996.