УДК: 004.056.53

С.М. Чуруброва

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ ІНФОРМАЦІЙНО-АНАЛІТИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДТРИМКИ ПРИЙНЯТТЯ ОРГАНІЗАЦІЙНИХ РІШЕНЬ

У статті описано політику безпеки інформації у системах підтримки організаційних рішень. Визначені основні вимоги захисту інформаційних об‘єктів, наведені особливості функціонування та інформаційні ресурси інтелектуальної інформаційної технології підтримки прийняття організаційних рішень. Розроблено загальні правила та вимоги розмежування та керування доступу на базі ABAC-моделі.
Ключові слова: захист інформації, політика безпеки, керування доступом, підтримка прийняття рішень.

Вступ

Фундаментальним поняттям захисту інформації є політика інформаційної безпеки. Політика безпеки (ПБ) викладає основні принципи, практичні рекомендації та вимоги, що закладаються в основу комплексної системи захисту інформації та спрямовані на захист інформації від критичних загроз [1, 2]. Зважаючи на технічні та програмно-апаратні проблеми, що виникають при організації захисту в інформаційних системах (ІС), у багатьох випадках достатній рівень безпеки досягається за рахунок вдало реалізованої ПБ. Тому розробка, дослідження та правильне застосування ПБ – це актуальна проблема сучасних систем захисту інформації [3].

Сучасна система підтримки прийняття рішень (СППР) це складна і динамічна система, яка враховує безліч факторів, тим більша потреба в гнучкості її підсистем [4, 5]. Одна з найважливіших підсистем захисту – це підсистема керування доступом основана на розподілі повноважень згідно з ПБ організації. Це ставить задачу розробки ПБ та моделі керування доступом, що мають властивості гнучкості, динамічності, простоти та адекватності системам керування корпоративним знанням та процесам підтримки прийняття рішень.

Мета даної статті полягає у визначенні загальних підходів та рекомендацій щодо розробки ПБ інтелектуальної інформаційної технології підтримки прийняття організаційних рішень (ІІТ ППОР) від загроз несанкціонованого доступу (НСД).

Особливості функціонування ІІТ ППОР

Загальними властивостями сучасних СППР є [4, 5]: інтегровані системи з комплексною архітектурою; дуже великі сховища даних; безліч одночасно працюючих користувачів; багаторазове використання; безліч джерел даних, включаючи мультимедіа та он-лайн дані; безліч форм доступу і оперування для користувачів; орієнтація на виконання завдань, вплив на ідентифікацію та прийняття рішень.

Дослідження [6] в середовищі автоматизованої підтримки організаційних рішень у сучасних організаціях показали, що особливостями функціонування ІІТ ППОР є:

– динамічність пріоритетів і контекстів;

– розподіленість необхідних знань про об’єкт управління серед представників різних бізнес-ролей;

– включення в число користувачів всіх осіб, безпосередньо або опосередковано впливають на якість і ефективність прийнятого рішення;

– необхідність активного використання всіх інформаційних ресурсів організації;

– максимальне використання контексту;

– критичність всіх етапів процесу прийняття рішення для його якості;

– а також необхідність збереження і поширення знань, набутих в процесі, для

подальшого семантично актуального доступу всіх отриманих результатів.

Загальні правила захисту інформації в ІІТ ППОР

Основними завданнями і метою захисту інформації в частині розмежування доступу є:

– забезпечення визначених політикою безпеки властивостей інформації (конфіденційності, цілісності, доступності) під час створення та експлуатації;

– обмеження кількості користувачів, що мають відношення до певної інформації при виконанні своїх функцій;

– реалізація правил розмежування доступу суб'єктів і їх процесів до даних;

– керування доступом користувачів до ресурсів ІС;

– зниження адміністративного навантаження в частині керування доступом.

Як складові частини загальної політики безпеки інформації ІІТ ППОР мають існувати політики забезпечення *конфіденційності* (гарантія, що інформація дається тільки авторизованим користувачам); *цілісності* (гарантія, що інформація не може бути несанкціоновано змінена); *доступності* (гарантія, що достовірна інформація буде доступна, коли це потрібно); та *спостережності* (забезпечення відповідальності користувача за свої дії і підтримки спроможності системи захисту виконувати свої функції) [7].

Інформація зберігає *конфіденційність*, якщо:

– дотримуються встановлені правила ознайомлення з нею;

– забезпечується керування потоками інформації від захищених об'єктів до користувачів;

– забезпечується повторне використання об'єктів;

– забезпечується захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Інформація зберігає *цілісність*, якщо:

– дотримуються встановлені правила її модифікації (видалення);

– забезпечується керування потоками інформації від користувачів до захищених об'єктів;

– забезпечується застосування стандартних підходів (різних стандартів і протоколів), що використовуються для безпечного обміну інформацією між системами;

– забезпечується захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище.

Інформація зберігає *доступність*, якщо:

– адміністратори мають можливість керувати використанням послуг і ресурсів;

– зберігається можливість ознайомлення з нею або її модифікації відповідно до встановлених правил упродовж будь-якого певного (малого) проміжку часу;

– реалізована можливість повернення системи у відомий захищений стан після відмови або переривання обслуговування.

Інформація зберігає властивість *спостережності*, якщо:

– реалізовано розподіл обов'язків, визначено ролі адміністратора та користувачів і притаманні їм функції;

– ідентифікація і автентифікація користувача, що намагається отримати доступ до системи, ідентифікація і автентифікація при обміні, автентифікація відправника, автентифікація отримувача;

– забезпечується достовірний канал;

– забезпечується цілісність комплексу засобів захисту;

– ведеться реєстрація дії, яка дозволяє контролювати небезпечні для системи дії.

Класифікація інформаційних ресурсів ІІТ ППОР

За режимом доступу інформація в ІІС ППОР має бути поділена на:

– відкриту;

– з обмеженим доступом.

Відкриту інформацію слід поділити на відкриту, яка не потребує захисту, або захист якої забезпечувати недоцільно, та відкриту, яка такого захисту потребує. До другої слід відносити інформацію, важливу для особи, суспільства і держави (відповідно до Концепції технічного захисту інформації в Україні), важливі для організації відомості, порушення цілісності або доступності яких може призвести до моральних чи матеріальних збитків та інші види інформації.

За правовим режимом інформація з обмеженим доступом має бути поділена на таємну та конфіденційну.

До таємної інформації мають бути віднесені будь-які відомості, що становлять державну таємницю (секретна інформація), а також відомості, що становлять іншу передбачену законом таємницю. Секретна інформація, в свою чергу, поділяється на категорії відповідно до Закону України «Про державну таємницю» [8].

Інформаційні об'єкти (об'єкти захисту) ІІТ ППОР

Структура інформаційної середи ІІТ ППОР визначає такі інформаційні об'єкти, що потребують захисту [6, 9]:

– централізовані бази та сховища даних;

– внутрішні інформаційні структури засобів автоматизації документів;

– локальні бази даних та документи підрозділів;

– ПАС – паспорти запозичених інформаційних об'єктів (є власними об'єктами ІС);

– онтологічна модель корпоративної архітектури;

– буферний сегмент онтологій (заповнюється системою у ході виявлення нових концептів і зв'язків);

– поле рішень: ретроспективні протоколи; протоколи відкритих, на даний час, процесів;

– контекстні бази даних (є сховищем інформації про зовнішні умови, що враховуються при прийнятті рішень);

– документи комунікацій;

– об'єкти підсистеми розмежування та керування доступом: репозиторії (сховища) атрибутів та політик; конфігураційна інформація.

Вимоги ПБ ІІТ ППОР

Окрім забезпечення конфіденційності, цілісності, доступності та спостереженості інформації ПБ ІІТ ППОР висуває наступні вимоги:

– більш гнучкий та динамічний контроль доступу до інформації та корпоративних знань. Надає можливість динамічної зміни повноважень, швидкої адаптації до непередбачуваних користувачів, максимального використовування контексту та багатомірності бізнес-правил;

– більш надійний контроль доступу до інформації та корпоративних знань. Дозволяє учасникам процесу прийняття рішень (ПР) знаходити та отримувати доступ до інформації необхідної для ПР, незалежно від домену та географії, не очікуючи більше заданого (прийнятного) часу;

– підтримка колаборативної роботи, спільних операцій та динамічних груп. Дозволяє командам ПР швидко обмінюватися інформацією та співпрацювати з зовнішніми учасниками, стейк-холдерами, для вироблення більш якісного рішення;

– застосування підходів SOA (сервісно-орієнтована архітектура). Використання різних стандартів та протоколів, зберігаючи при цьому сумісність та узгодженість операцій;

– гарантії доступності корпоративних ресурсів. Гарантує, що термінали, комунікації, інформаційні системи та корпоративні сервіси залишаються доступними для користувачів для забезпечення потреб за запитом;

– зниження вимог до кадрових ресурсів. Перенаправлення робочих сил з адміністрування та керування технологіями, шляхом зниження адміністративного навантаження в частині керування, підтримки запитів та інформаційної безпеки за рахунок автоматизації обробки запитів.

Правила розмежування доступу в ІІТ ППОР

Основою ПБ ІІТ ППОР є модель керування доступом на основі атрибутів (атрибутивна модель керування доступом, ABAC) [5].

ABAC – логічна модель контролю доступу, де рішення про надання доступу суб'єкта до об'єкта приймається на основі привласнених атрибутів суб'єкта, об'єкта, середовищем їх функціонування (контексту) на момент запиту і набору політик, що визначають припустимі операції для суб'єкт-об'єктних комбінацій атрибутів. Елементи матриці доступу не зберігається в явному вигляді, а динамічно обчислюються при кожній спробі доступу для конкретної пари суб'єкт-об'єкт на основі їх атрибутів. Крім економії пам'яті досягається несуперечливість бази даних захисту, а також зручність її адміністрування.

Атрибутивна модель керування доступом є найбільш універсальною [4]. Вона покликана подолати обмеження домінуючих моделей доступу (DAC, MAC і RBAC), одночасно об'єднавши їх переваги [10]. Використовуючи ABAC, можна емулювати дискреційне, мандатне і рольове керування доступом. Це дуже важливо, оскільки можна розробляти системи, що підтримують ABAC і конфігурувати їх у разі потреби для реалізації DAC, MAC або RBAC.

Для забезпечення необхідного рівня безпеки інформації в ІІТ ППОР має виконуватися наступне:

– всі суб'єкти і об'єкти системи мають бути однозначно ідентифіковані (кожному об'єкту всередині системи і кожному суб'єкту, який використовує систему, повинні бути присвоєні особливі атрибути, що його характеризують);

– визначено набір ролей у системі (у даному випадку це не всі ролі суб'єктів організації, а тільки ролі учасників процесу прийняття рішень, як головного концепту ІІТ ППОР, необхідні для визначення динамічних прав доступу);

– права доступу суб'єкта до об'єкта системи визначаються на основі наданих атрибутів суб'єкта, наданих атрибутів об'єкта, контексту та набору політик, що визначають припустимі операції для суб'єкт-об'єктних комбінацій атрибутів;

– кожному об'єкту системи відповідає хоча б одна політика, що задає правила доступу;

– механізм реалізації контролю доступу має містити можливість санкціонованої зміни правил розмежування доступу та керування атрибутами;

– право зміни правил розмежування доступу надається тільки виділеним суб'єктам.

За наявності таємної інформації:

– задано атрибути, що відповідають лінійно упорядкованому набору міток таємності;

– у системі мають бути реалізовано мандатний принцип контролю читання та запису (набір політик).

Розмежування доступу в ІІТ ППОР може здійснюватись за наступними параметрами:

– вид інформаційного об'єкта, тематика, призначення, бізнес-функціональність, оргструктурна приналежність, авторство, семантична категорія, ступінь важливості та секретності інформації;

– умовами обробки: час обробки, планова прив'язка, технологічні процеси (ті, що створюють, ті, що використовують інформацію; ті, що ініціюють інформаційні процеси) і т. ін.

При розгортанні в масштабі підприємства для збільшення обміну інформацією між різними організаціями, реалізація ABAC вимагає інфраструктури керування атрибутами, політики безпеки програмною мовою, а також у доповнення до основної політики, атрибутів і вимогам механізму контролю доступу, підприємство має підтримувати функції керування для розробки і розподілу політики підприємства, атрибутів суб'єкта, атрибутів об'єктів, розгортання і поширення механізму контролю доступу.

Ці фактори можуть бути зведені навколо комплексу заходів:

– встановити економічне обґрунтування для реалізації АВАС;

– визначити експлуатаційні вимоги та архітектуру підсистеми АВАС підприємства;

– створити або удосконалити бізнес-процеси для підтримки АВАС;

– розробити і придбати сумісний набір можливостей АВАС.

Гарантії АВАС-атрибутів

Загальні властивості АВАС щодо атрибутів, як основи системи авторизації, діляться на три категорії [11] (таблиця):

– *точність* встановлює політику та технічні основи для семантично і синтаксично правильного використання цих атрибутів і умов навколишнього середовища, а також гарантує, що заявлені атрибути заслуговують довіри;

– *цілісність* бере до уваги різні стандарти і протоколи, що використовуються для безпечного обміну атрибутами між системами, для того, щоб уникнути порушення цілісності та конфіденційності атрибутів;

– *доступність* полягає у тому, що постачальник атрибутів гарантує приймаючій стороні можливість оновлення і витягу атрибутів зі сховища. Крім того мають бути розглянуті можливості резервного копіювання та відмовостійкості сховища атрибутів. Зверніть увагу, що деякі атрибути можуть змінюватися регулярно або протягом довгого часу.

Таблиця. Рівні гарантій атрибутів АВАС

Рівні гарантій	Точність	Цілісність	Доступність
1	Атрибути належним чином перевірені на достовірність під час постачання та керування	Безпечне сховище атрибутів. Безпечний обмін даними між ПА та приймаючою стороною (ПС)	Частота оновлення атрибутів відповідає вимогам продуктивності системи
2	*Включає в себе 1рівень.* Задокументовані правила та/або стандарти для присвоєння значень та визначень атрибутів (синтаксичні та семантичні правила)	*Включає в себе 1рівень.* Виділенні сховища (репозиторії) атрибутів	*Включає в себе 1рівень.* Кешування атрибутів під час роботи за вимогами продуктивності системи
3	*Включає в себе 2 рівень.* Атрибути охоплюють усі вимоги політики інформаціонної безпеки організації	*Включає в себе 2 рівень.* Зашифровані значення атрибутів і зв’язку між ПА и ПС	*Включає в себе 2 рівень.* Підтримка резервного копіювання атрибутів
4	*Включає в себе 3 рівень.* Централізоване або об‘єднане управління атрибутами	*Включає в себе 3 рівень.* Формальні правила або політики (чи стандарти) для створення, оновлення, зміни та видалення атрибутів	*Включає в себе 3рівень.* Логування при зміні атрибутів і прав доступу

Постачальником атрибутів (ПА) є будь-яка особа або система, яка забезпечує суб'єкт, об'єкт (або ресурс), або стан навколишнього середовища атрибутами незалежно від способу передачі.

ПА може бути оригінальним авторитетним джерелом або отримувати інформацію з авторитетного джерела для перепакування та зберігання-і-передачі до системи АВАС. Значення атрибутів можуть генеруватися людиною (наприклад, бази даних співробітників) або отримана з формул (наприклад, рахунок кредиту).

Незалежно від джерела атрибута, система повинна гарантувати, що значення атрибута, отриманого від ПА точно пов'язано з суб'єктом, об'єктом чи станом навколишнього середовища, до якого він належить.

У таблиці наведені приклади рівнів гарантії атрибутів АВАС на основі властивостей точності, цілісності та доступності.

Висновки

В даній роботі описано політику безпеки ІІТ ППОР щодо збереження конфіденційності, цілісності, доступності та спостережності інформації. Визначені основні вимоги захисту інформаційних об'єктів, наведені особливості функціонування та інформаційні ресурси ІІТ ППОР. Розроблено загальні правила та вимоги розмежування та керування доступу на базі АВАС-моделі.

Вище викладені загальні правила, вимоги, особливості функціонування та ін. орієнтовані на полегшення розгортання підсистеми захисту інформації в таких складних і динамічних сучасних системах як системи інтелектуальної інформаційної технології підтримки прийняття організаційних рішень.

1. *Термінологія* в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. – К.: ДСТСЗІ СБ України, 1999. – 26 с.
2. *Типове* положення про службу захисту інформації в автоматизованій системі: НД ТЗІ 1.4-001-2000. – К.: ДСТСЗІ СБ України, 2000. – 26 с.
3. *Антонюк А.О.* Політика безпеки інформації в захищених автоматизованих системах // Наукові записки НаУКМА. Комп'ютерні науки. – 2003. – Том 21. – С. 102–107.
4. *Power D.J.* What is a modern decision support system? [Електронний ресурс]: article Prof. 27.12.2007. DSSResources.COM // – Режим доступу: http://dssresources.com/faq/index.php?action=artikel&id=154
5. *Чуруброва С.Н.* Обоснование модели управления доступом в системах поддержки организационных решений // Сучасний захист інформації. – 2015. – № 2. – С. 64–71.
6. *Ильина Е.П.* Принципы построения интеллектуальной информационной технологии поддержки решений в организации // Проблеми програмування. – 2015. – № 2. – С. 63–75.
7. *Загальні* положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-002-99. – К.: ДСТСЗІ СБ України, 1999. – 16 с.
8. *Закон* України "Про державну таємницю" від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93. (В редакції Закону N 1079-XIV від 21.09.99).
9. *ДР* 0112U002763. Звіт про НДР "Розробка методів, технологій та засобів інформаційно-аналітичного забезпечення підтримки прийняття рішень в системах організаційного управління" (проміжний). – ІПС НАНУ, 2014. – 141 с.
10. *Xin J., Ram Krishnan and Ravi Sandhu.* A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. - 26th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSEC). – 2012. – pp. 41-55.
11. *Hu Vincent C., D. Richard Kuhn, and David F. Ferraiolo.* "Attribute-Based Access Control." IEEE Computer 48.2. – 2015. – P. 85–88.

References

1. Terminology in the field of information security in computer systems from unauthorized access: RD TPI 1.1-003-99. — K.: SSSCIP of Ukraine, 1999. – 26 p.
2. Standard provision of security services in automated systems: RD TPI 1.4-001-2000. — K.: SSSCIP of Ukraine, 2000. – 26 p.

3. Antoniuk A. Security policy information in secure automated systems [In Ukranian] In: Scientific notes NaUKMA. – 2003. – Vol. 21, Computer Science. – P. 102–107.
4. Power D.J. What is a modern decision support system? [Electronic resource]: article Prof. Daniel J. Power, 27.12.2007. DSSResources.COM // – Access mode: http://dssresources.com/faq/index.php?action=artikel&id=154
5. Churubrova S. Substantiation of access control model in the support system of organizational decisions [In Rassian] In: *Modern Information* Security . – 2015. – N 2. – P. 64–71.
6. Ilina E.P., Sinitsyn I.P., Yablokova T.L. Designing principles of the Intelligent information technology for organization decisions [In Rassian] In: Problems in programming. – 2015. – N 2. – P. 63–75.
7. General provisions for the protection of information in computer systems against unauthorized access: RD TPI 1.1-002-99. — K.: SSSCIP of Ukraine, 1999. – 16 p.
8. Law of Ukraine "On State Secrets" dated 21 January 1994 N 3856-XII // Bulletin of the Supreme Council of Ukraine. – 1994. – N 16. – P. 93.
9. SR 0112U002763. Research report "Development of methods, technologies and information and analytical support of decision support systems in organizational management" (intermediate) – ISS NASU, 2014. – 141 p.
10. Xin J. A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC. / Xin Jin, Ram Krishnan and Ravi Sandhu. - 26th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy (DBSEC). – 2012. – P. 41–55.
11. Hu, Vincent C., D. Richard Kuhn, and David F. Ferraiolo. "Attribute-Based Access Control." IEEE Computer 48.2. – 2015. – P. 85–88.

Одержано 13.09.2016

Про автора:

Чуруброва Світлана Миколаївна,
аспірантка ІПС НАНУ,
інженер-програміст 1 кат.
Кількість наукових публікацій
в українських виданнях – 4.
http://orcid.org/0000-0002-7106-1199.

Місце роботи автора:

Інститут програмних систем НАН України,
03187, Київ-187,
проспект Академіка Глушкова, 40.
Тел.: 526 5553.
E-mail: s4urubrova@gmail.com